The trust of German companies in U.S. cloud providers from the perspectives of buyers and sellers

Sven Gerritsen

A thesis submitted to

The University of Gloucestershire

in accordance with the requirements of the degree of

Doctorate in Business Administration (DBA)

in the Business School

January 2020

Abstract

Building and maintaining successful business relationships between buyers and sellers continues to be of key interest for sales organisations and academics. The positive effect of trust on the buyer's purchasing behaviour has been proven in multiple studies in the past. However, the digitalisation of business processes and the globalisation of products and services require an additional perspective on this matter.

Cloud computing is about to radically change the way that businesses purchase and utilize information technology. It is a catalyst for the disruption of existing business models and for the creation of new products and services. Amongst the various cloud computing deployment models, public cloud computing offers the most benefits for businesses including low investment costs, almost unlimited scalability and multi-geographical availability of IT services. Today, the most advanced public cloud computing services are offered by U.S. technology companies.

U.S. cloud providers are, however, subject to U.S. laws and were suspected of allowing the U.S. government to force businesses that have their headquarters in the U.S. to hand over user data to U.S. government authorities, even if the data is stored in a data centre in the EU. The fact that U.S. cloud providers could be forced to disclose private and confidential data to the U.S. government emerged as one of the top concerns among IT managers of German companies. In addition to these legal complications, the disclosures by Edward Snowden around the global surveillance programmes of the U.S. National Security Agency (NSA) have caused significant distrust of German companies in U.S. cloud services.

The objective of the current research was to analyse the perspective of the buyers and sellers on the importance of the concept of trust for German companies for the adoption of public cloud computing services from U.S. cloud providers (RO1a) and on the impact of the cultural differences between Germany and the U.S. (RO1b) as well as the influence of the sector of a German company on trust and public cloud adoption (RO1c). The second objective was to explore the trust relationship between German companies and U.S. cloud products (RO2a), U.S. cloud provider companies (RO2b), the local sales representatives of the U.S. cloud providers (RO2c) and the U.S. government (RO2d). In addition to these theoretical contributions, this study made a contribution to practice by offering some important insights into how U.S. cloud

providers can improve their trust relationship with German companies (RO3) and developed a conceptual framework for buyer-seller trust in the context of international public cloud computing services (RO4).

A qualitative research methodology was adopted to provide a deep understanding of the properties and the underlying reasons for the (dis-)trust of the key respondents. Semi-structured interviews were conducted for the collection of dyadic data with key informants from German companies from different sectors (buyers) and local sales representatives of U.S. cloud providers (sellers). By applying a constructivist worldview, the findings from this study made several contributions to existing knowledge.

Firstly, the present study provides additional evidence with respect to the importance of trust in buyer-seller relationships by demonstrating that trust is a vital component for German companies for adopting public cloud computing services from U.S. cloud providers. This trust is influenced by the cultural background of the buyer and seller as well as the sector the buying company is operating in.

Secondly, the current findings add to a growing body of literature on buyer-seller trust including inter-organisational trust, inter-personal trust, product trust and by introducing an additional trust relationship named foreign government trust. This study has demonstrated, for the first time, that foreign government trust had a stronger impact on the buyer's purchasing behaviour than the three other trust relationships.

Thirdly, the empirical findings in this study provide a new understanding of the measures that U.S. cloud providers can take to enhance the trust of their German customers. This includes building cloud data centres in Germany, legal proceedings against the U.S. government, improved cloud computing contracts and strong data encryption standards.

Keywords: Trust, buyer-seller relationships, cloud computing, German companies, U.S. cloud providers, national culture, company trust, salesperson trust, product trust, foreign government trust, global surveillance disclosures

Declaration

I declare that the work in this thesis was carried out in accordance with the regulations of the University of Gloucestershire and is original except where indicated by specific reference in the text. No part of the thesis has been submitted as part of any other academic award. The thesis has not been presented to any other education institution in the United Kingdom or overseas.

Any views expressed in the thesis are those of the author and in no way represent those of the University.

Signed: Date: 24/01/2020

DOI 10.46289/YHPG2720

Acknowledgement

There are many people who have supported me during my research work and I would like to express my gratitude to all those who helped me to complete this thesis.

First and foremost, I want to thank my first supervisor Dr Elke Pioch and my second supervisor Dr Adele Carter for their advice, insights and extensive feedback. I also want to thank my examiners, Dr Rana Tassabehji and Dr Stuart Hanmer-Lloyd, who gave me very insightful comments on this thesis which helped to improve the final version.

Furthermore, I would like to offer my special thanks to all key respondents from the German companies and the U.S. cloud providers for participating in this study and for investing time and effort in the interviews.

I would also like to thank my fellow doctoral students for their feedback, cooperation and of course friendship. I am particularly grateful for the support and encouragement from Dr Matthias Paus. Additionally, I wish to thank Dr Eva Niemann who helped me to believe in myself and supported me with the final steps of the research process.

Moreover, I am deeply grateful to my parents and my brother for pushing me through my first years of school and for always being there for me. I am also most grateful to my friends who have supported me along the way. A special thanks goes to the Moon family for all the constructive discussions and warm encouragements.

My deepest appreciation goes to my beloved wife Sofie for her untiring patience with me and for cheering me up during difficult times. Without her encouragement and persistent support, this research would not have been possible.

This thesis is dedicated to our son Nils, born on the 20th of August 2015 and our daughter Linn, born on the 7th of February 2018.

Table of contents

Abstract ... ii
Declaration ... iv
Acknowledgement ... v
Table of contents ... vi
List of figures ... x
List of tables ... xi
List of abbreviations and acronyms ... xii
1 Introduction ... 1
1.1 Problem statement ... 2
1.2 Research aim ... 4
1.3 Research objectives ... 5
1.4 Scope and limitations ... 5
1.5 Personal interest ... 5
1.6 Thesis structure ... 7
2 Background ... 9
2.1 Cloud computing ... 10
2.1.1 Terminology ... 11
2.1.2 Basic concepts ... 14
2.1.3 Business benefits of public cloud computing ... 18
2.1.4 U.S. cloud provider ... 22
2.1.5 German cloud consumer ... 23
2.1.5.1 German history and culture ... 26
2.1.5.2 Economic espionage ... 27
2.1.6 Concerns about public cloud computing ... 28
2.1.6.1 Security ... 32
2.1.6.2 Privacy ... 33
2.1.6.3 Regulations, policies and legal issues ... 37
2.2 Global surveillance disclosures ... 39
2.2.1 Pre-Snowden (2001-2013) ... 40
2.2.2 Post-Snowden (2013-present) ... 44
2.3 A matter of trust ... 47
2.3.1 Government reactions ... 47
2.3.2 German company reactions ... 54
2.3.3 U.S. cloud provider reactions ... 57
2.3.4 German cloud provider reactions ... 62
2.4 Summary ... 64
3 Literature review ... 66
3.1 Importance of trust ... 67
3.2 Definitions of trust ... 69
3.2.1 Definitions of trust by philosophers ... 69

3.2.2 Definitions of trust by sociologists 71
3.2.3 Definitions of trust by economists 73
3.2.4 Definitions of trust for this study 77
3.3 Buyer-seller trust 78
3.3.1 Inter-organisational and interpersonal trust 80
3.3.2 Individual components of trust 81
3.4 Trust relationships 83
3.4.1 Trust in the selling company 83
3.4.2 Trust in the salesperson 87
3.4.3 Trust in the product 94
3.5 Trust in cloud computing 96
3.6 The role of culture 106
3.6.1 Culture and trust 107
3.6.2 Cultural differences between Germany and the U.S. 109
3.6.3 Models of national culture 113
3.6.4 Hofstede's cultural dimensions 116
3.7 Research gaps 119
3.7.1 Importance of trust 119
3.7.2 Trust relationships 121
3.7.3 How U.S. cloud providers can improve the trust in their services 126
3.8 Summary 127
4 Research design 129
4.1 Research paradigm 130
4.1.1 Constructivism 130
4.1.2 Justification 131
4.2 Research methodology 133
4.2.1 Qualitative research 134
4.2.2 Justification 134
4.3 Research method 135
4.3.1 Qualitative interviews 136
4.3.2 Justification 136
4.4 Data collection 137
4.4.1 Key informants 138
4.4.2 Semi-structured and open-ended questions 139
4.4.3 Interview skills 140
4.4.4 Interview guide 142
4.4.5 Interview participants 144
4.4.5.1 Interviews with German cloud consumer companies 145
4.4.5.2 Interviews with U.S. cloud provider companies 148
4.4.5.3 Sample size 149
4.4.6 Pilot interview 150

4.5 Data analysis 151
4.5.1 Transcription 153
4.5.2 Generating initial codes 154
4.5.3 Searching for themes 155
4.5.4 Reviewing themes 156
4.5.5 Defining and naming themes 157
4.5.6 Producing the report 158
4.6 Role of the researcher 159
4.7 Ethical considerations 161
4.8 Summary 162
5 Findings 163
5.1 Importance of trust 163
5.2 Cultural differences 165
5.3 Sector 171
5.4 Cloud computing technology 173
5.5 U.S. cloud services, features and maturity 175
5.6 Shadow IT 177
5.7 U.S. cloud providers 179
5.8 German cloud providers 182
5.9 Private cloud 184
5.10 Local sales representatives 187
5.11 Market and sector knowledge 189
5.12 Global surveillance disclosures 191
5.13 Economic espionage 194
5.14 U.S. government reactions 196
5.15 German and EU government reactions 198
5.16 Data centre location 201
5.17 Legal proceedings 203
5.18 Cloud computing contracts 204
5.19 Data encryption 206
5.20 Summary 207
6 Discussion 213
6.1 Importance of the concept of trust for cloud adoption (RO1) 214
6.1.1 Importance of trust (RO1a) 214
6.1.2 Impact of the cultural differences (RO1b) 216
6.1.2.1 Individualism 217
6.1.2.2 Uncertainty avoidance 221
6.1.2.3 Long-term orientation 228
6.1.2.4 Indulgence 229
6.1.2.5 History 231
6.1.2.6 Age 232

6.1.3 Influence of the sector (RO1c) 235
6.1.4 Summary 241
6.2 Trust relationships (RO2) 242
6.2.1 Product trust (RO2a) 242
6.2.1.1 Cloud computing technology 242
6.2.1.2 U.S. cloud services 244
6.2.1.3 Shadow IT 246
6.2.1.4 Summary 247
6.2.2 Company trust (RO2b) 248
6.2.2.1 U.S. cloud providers 249
6.2.2.2 German cloud providers 252
6.2.2.3 Private cloud 256
6.2.2.4 Summary 260
6.2.3 Salesperson trust (RO2c) 261
6.2.3.1 Local sales representatives 261
6.2.3.2 Market and sector knowledge 267
6.2.3.3 Summary 275
6.2.4 Foreign government trust (RO2d) 276
6.2.4.1 Global surveillance disclosures 276
6.2.4.2 Economic espionage 280
6.2.4.3 U.S. government reactions 284
6.2.4.4 German and EU government reactions 286
6.2.4.5 Summary 289
6.3 How U.S. cloud providers can improve the trust relationship (RO3) 289
6.3.1 Data centre location 290
6.3.2 Legal proceedings 293
6.3.3 Cloud computing contracts 295
6.3.4 Data encryption 298
6.4 Conceptual framework (RO4) 300
7 Conclusions 304
7.1 Contribution to knowledge 305
7.2 Contribution to practice 318
7.3 Limitations and recommendations for future research 323
8 References 324
Appendix 1: “Interview questions” 380
Appendix 2: “Participant recruitment” 386
Appendix 3: “Coding and notes writing” 389
Appendix 4: “Additional quotes” 392

List of figures

Figure 1: Introduction chapter 1
Figure 2: Thesis structure 7
Figure 3: Background chapter 9
Figure 4: Cloud consumer and provider relationship. Adapted from Erl et al. (2013, p. 52). 13
Figure 5: Cloud essential characteristics, service models and deployment models 14
Figure 6: Cloud computing service models. Adapted from Harms and Yamartino (2010). 17
Figure 7: Use of cloud computing services in the EU. Adapted from Eurostat (2017). 24
Figure 8: Cloud usage by sector. Adapted from Techconsult (2012) 25
Figure 9: Privacy and data protection by country. Adapted from Forrester (2017). 36
Figure 10: Respondents that heard about Edward Snowden. Adapted from CIGI-Ipsos (2014). 56
Figure 11: Literature review chapter 66
Figure 12: Components of trust according to Plank et al. (1999). 82
Figure 13: The six dimensions of national culture. Adapted from Hofstede (2018). 118
Figure 14: Foreign government trust 124
Figure 15: Research design chapter 129
Figure 16: Cloud usage by sector. Adapted from KPMG (2016). 236
Figure 17: Cloud risks before and after Snowden. Adapted from PwC (2013b, p. 19). 279
Figure 18: Types of data German companies keep on premises. Adapted from Mureșan (2016). 282
Figure 19: Location of most-trusted cloud computing providers. Adapted from Mureșan (2016). 291
Figure 20: Location of least-trusted cloud computing providers. Adapted from Mureșan (2016). 292
Figure 21: Conceptual framework 301
Figure 22: Conclusions chapter 304

List of tables

Table 1: Cloud computing roles. Adapted from F. Liu et al. (2011, p. 4). 13
Table 2: Essential cloud computing characteristics. Adapted from NIST (2011b). 15
Table 3: Cloud computing service models. Adapted from (NIST, 2011b, p. 2). 16
Table 4: Cloud computing deployment models. Adapted from (NIST, 2011b, p. 3). 18
Table 5: Top 10 cloud providers in Europe. Adapted from European Commission (2015b). 22
Table 6: Top 10 cloud computing risks. Adapted from Dutta et al. (2013). 29
Table 7: Cloud barriers in Europe. Adapted from European Commission (2012c, p. 34). 30
Table 8: Top 5 concerns, obstacles and risks for German companies 30
Table 9: Timeline of laws and bills regarding the U.S. government surveillance activities 42
Table 10: Timeline of global surveillance disclosures 45
Table 11: Timeline of government reactions 51
Table 12: Timeline of U.S. cloud provider reactions 59
Table 13: Summary of key definitions of trust by philosophers 70
Table 14: Definitions of trust by sociologists. 72
Table 15: Summary of key definitions of trust by economists 74
Table 16: Literature on inter-organisational company trust 84
Table 17: Literature on salesperson trust 88
Table 18: Literature on product trust 94
Table 19: Literature on trust in cloud computing 100
Table 20: Interviews with German companies 147
Table 21: Interviews with U.S. cloud providers 148
Table 22: List of themes 157
Table 23: Research objectives and themes 158
Table 24: Properties of sectors included in the current research 237

List of abbreviations and acronyms

Abbreviation or acronym	Description
BDSG	Bundesdatenschutzgesetz (English: German Federal Data Protection Act)
BfDI	Bundesbeauftragte(r) für den Datenschutz und die Informationsfreiheit (English: Federal Commissioner for Data Protection and Freedom of Information)
BSI	Bundesamt für Sicherheit in der Informationstechnik (English: German Federal Office for Information Security)
BYOD	Bring your own device
CAPEX	Capital expenditure
CEBR	Centre for Economics and Business Research, London, UK
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CIO	Chief Information Officer
CSA	Cloud Security Alliance
CRM	Customer Relationship Management
DOJ	U.S. Department of Justice
DPD	Data Protection Directive of the European Union
EC	European Commission
ECPA	Electronic Communications Privacy Act
EEA	European Economic Area
ENISA	European Network and Information Security Agency
EP	European Parliament
EU	European Union
FAQ	Frequently asked questions
FBI	U.S. Federal Bureau of Investigations
GCHQ	British Government Communications Headquarters
GDPR	EU General Data Protection Regulation
HP	Hewlett-Packard Company
IaaS	Infrastructure as a Service
IBM	International Business Machines Corporation
ICT	Information and communications technology
IDC	International Data Corporation
IT	Information Technology
ITA	U.S. International Trade Administration
ITIF	Information Technology and Innovation Foundation
DMS	Document Management System
NIST	U.S. National Institute of Standards and Technology
NSA	U.S. National Security Agency
NSL	National Security Letter
OJP	U.S. Office of Justice Programs
OPEX	Operational expenditure
OSI	Open Systems Interconnection model
PaaS	Platform as a Service
SaaS	Software as a Services
SLA	Service Level Agreement
SME	Small and Medium Enterprise
TCO	Total cost of ownership
TTIP	Transatlantic Trade and Investment Partnership
U.S.	United States (of America)
UN	United Nations
USA	United States of America
USA PATRIOT Act	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act

1 Introduction

The purpose of this chapter is to establish the context of the research topic and to explain the structure of the thesis (see Figure 1). Section 1.1 provides a brief overview of the importance of this study for the society and for the discipline and highlights the research problem. The chapter continues with giving a brief synopsis of existing literature and highlighting a knowledge gap in the field of study.

The next section (1.2) will state the aim of this research and indicate the areas where this study makes a unique and original contribution. This is followed by the objectives of this research (1.3).

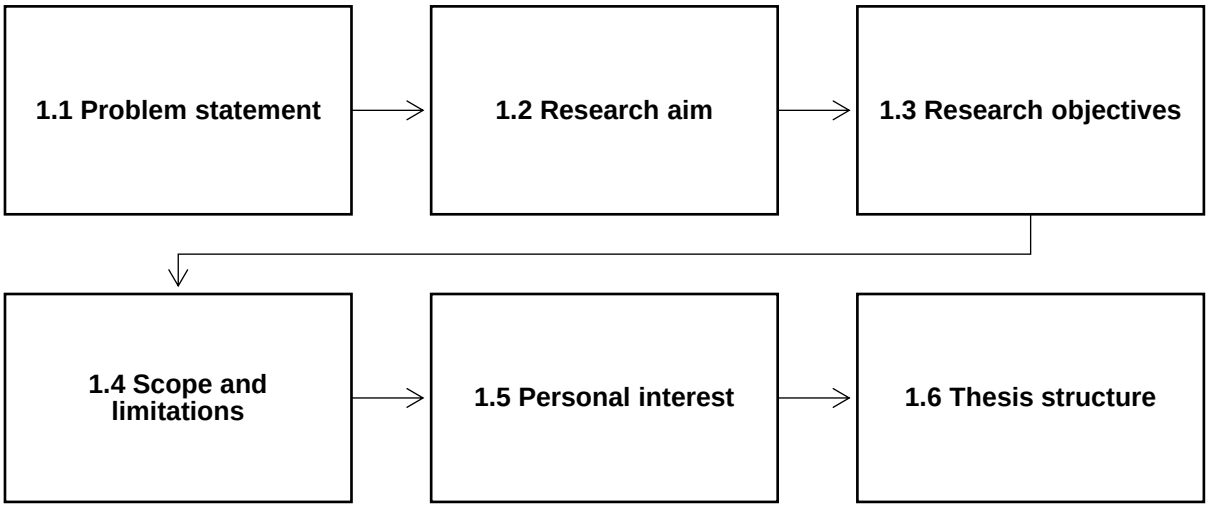


Figure 1: Introduction chapter

Section 1.4 gives an overview of the scope and limitations of this study and Section 1.5 explains reasons for my personal interest in this topic.

The last section (1.6) will provide an overview of the overall structure of the thesis.

1.1 Problem statement

The past decade has seen rapid advances in the field of cloud computing, and it is becoming increasingly difficult to ignore the impact of cloud computing technologies on businesses of all sizes and industries. According to leading market research organisations, cloud computing is one of the top global technology trends of the next years (Forrester, 2016; Gartner, 2016; IDC, 2016; McKinsey, 2016) and for more than half of all companies in Germany, cloud computing is a formal part of their IT or corporate strategy (IDC, 2017; KPMG, 2017b).

Businesses have the choice between different cloud computing deployment models (Goyal, 2014), of which public cloud computing offers the most economic benefits in terms of economies of scale, scalability and performance (Domnik, 2015; KPMG, 2012). However, German companies have one of the lowest cloud computing adoption rates in the EU (Eurostat, 2017) and also in comparison with many other industrialized countries in the world. The rapid changes in technology are having a considerable effect on international business relationships. In the new global economy, cloud computing services can be offered and consumed from anywhere on the planet. Today, the most advanced and most popular public cloud computing solutions are offered by U.S. cloud providers such as Amazon, Google and Microsoft (Büst, 2016; Castro, 2013; Experton, 2012; Herrmann, 2017; Millard, 2013; Schechner, 2016).

These U.S. cloud providers are, however, subject to U.S. laws and were suspected of allowing the U.S. government to force businesses that have their headquarters in the U.S. to hand over user data to U.S. government authorities, even if the data was stored in a data centre in the EU (Van Hoboken, Arnbak, & Van Eijk, 2012). The fact that U.S. cloud providers could be forced to disclose private and confidential data to the U.S. government emerged as one of the top concerns among IT directors of companies in the EU and received considerable critical attention (Overby, 2012; Taylor, 2011). In Germany, companies were particularly worried about potential privacy and data protection issues in connection with the USA PATRIOT Act (Experton, 2012; PwC, 2013a).

The disclosures by Edward Snowden around the global surveillance programmes of the U.S. National Security Agency (NSA) and its international partners have presumably reinforced these concerns (Naughton, 2013; Traynor, 2013) and fuelled

the debate about the question if German companies could trust U.S. cloud providers (AP, 2013). Insufficient trust was thereupon mentioned as one of the major obstacles to public cloud computing adoption by EU and German politicians and German companies (Mascolo & Scott, 2013; Schneier, 2013; Smale, 2013; Stiglitz, 2013).

Trust is, however, “essential for stable social relations” (Blau, 1964, p. 99) and a “functional necessity for society” (Lewis & Weigert, 1985a, p. 456). In buyer-seller relationships, trust is a major area of interest within the field. It is a vital component for commercial transactions (Sako, 1998) and “supplier firms must make significant investments to develop and maintain customer trust” (Doney & Cannon, 1997, p. 48). More importantly, low trust environments reduce investments and can considerably reduce market efficiency (Zak & Knack, 2001).

Although there is an extensive amount of literature available on trust in buyer-seller relationships (Arnott, 2007; Huth, 2004), there are several gaps in the literature that need to be addressed. Firstly, no previous study has investigated the importance of trust for German companies for the adoption of public cloud computing services from U.S. cloud providers. This includes the impact of the cultural differences between Germany and the U.S. and the influence of the sector of a German company on trust and public cloud adoption.

Secondly, there has been considerable research on the trust relationships between the buyer and the selling company, the buyer and the salesperson and the buyer and the product or service. However, these trust relationships have not been explored in the context of U.S. public cloud services and German companies. Moreover, the practitioner literature suggests that there is at least one additional relationship that plays a key role in the trust of German companies in U.S. cloud services. This fourth relationship that could be called foreign government trust requires further research.

Thirdly, there is increasing concern by the U.S. cloud providers about losing business in European countries such as Germany because of trust issues. No research has been found that addressed this concern by identifying ways that U.S. cloud providers could improve the trust of German companies in their public cloud services. These three gaps identified in the literature led to the aim and objectives of the current research which will be described in the following sections.

1.2 Research aim

The aim of this research is to contribute to the understanding of trust in buyer-seller relationships in the context of international cloud computing services by exploratory research on the trust relationships between German companies and U.S. cloud providers from the perspectives of buyers and sellers.

There are two key areas where this study should make a unique and original contribution. Firstly, the findings should make an important contribution to the field of trust in buyer-seller relationships. A key outcome of this research is an analysis of the importance of the concept of trust for German companies for the purchase of cloud computing services from U.S. cloud providers. This includes the impact of the cultural differences between Germany and the U.S. as well as the influence of the sector of a German company on trust and public cloud adoption. Another aim is the exploration of the influence of the trust relationships between the German companies and a) U.S. cloud products, b) U.S. cloud provider companies, c) the local sales representatives of the U.S. cloud providers and d) the U.S. government. Additionally, the current research should produce a conceptual framework that illustrates the trust influence factors and relationships.

Secondly, in addition to these theoretical contributions, the study should make a contribution to practice by offering some important insights into how U.S. cloud providers can improve their trust relationship with German companies. This study will address the managerial implication of this buyer-seller trust relationship from the point of view of U.S. public cloud service providers by identifying ways to improve the trust of German companies in their services and eventually grow their public cloud computing business in Germany.

1.3 Research objectives

This study aimed to address the following research objectives:

1. Analyse the perspective of the buyers and sellers on
    a. the importance of trust for German companies for the adoption of public cloud computing services from U.S. cloud providers (RO1a),
    b. the impact of the cultural differences between Germany and the U.S. on trust and public cloud adoption (RO1b) and
    c. the influence of the sector of a German company on trust and public cloud adoption (RO1c).
2. Explore the trust relationship between German companies and
    a. U.S. cloud products (RO2a),
    b. U.S. cloud provider companies (RO2b),
    c. the local sales representatives of the U.S. cloud providers (RO2c) and
    d. the U.S. government (RO2d).
3. Identify ways how U.S. cloud providers can improve the trust relationship with German companies (RO3).
4. Develop a conceptual framework for buyer-seller trust in the context of international public cloud computing services (RO4).

1.4 Scope and limitations

The scope of this research is limited to the trust relationship between German companies and U.S. cloud providers. It is beyond the scope of this study to examine the trust relationship between buyers and sellers from other countries or other types of businesses.

A full discussion of the limitations of the present study is presented in Section 7.3 of this study.

1.5 Personal interest

Following the recommendation of APA (2013), to avoid ambiguity, I used a personal pronoun rather than the third person when describing decisions made or steps taken in my research. This is also in line with the constructivism paradigm applied to the current research, which acknowledges the fact that the researcher plays an active role in the research process.

Although this project was conceived during my time working for Microsoft Germany, my main reason for choosing this topic was personal interest. I became interested in the role of the concept of trust in cloud computing adoption after reading about the theoretical possibility of the U.S. government to access data stored in other countries and the associated concerns of German companies. As an IT professional, I witnessed the development of the cloud computing industry and it was my experience of working with clients from different industries that has driven this research. My role as a researcher is further explained in Section 4.6 of this research.

Interestingly, the global surveillance programmes of the U.S. National Security Agency (NSA) and its international partners were only disclosed during this research. Before the revelations by Edward Snowden, the topic around the impact of U.S. law on cloud computing services was only discussed between subject matter experts in IT and legal communities. However, after the extensive press coverage of this topic, large parts of the population knew about the surveillance activities. I could therefore assume that my interview respondents had dealt with this subject and had an opinion about it.

According to my personal assessment, my interest in the topic did not have a considerable distorting effect on the outcomes of the current research. The research questions and interview questions were derived from the practitioner and academic literature in the field and the findings were based on the answers of the interviewees. However, as a constructivist researcher, my position, experience, perspective and interactions were part of the research process and all conclusions are consequently interpretive. For this reason, I needed to practice ongoing self-reflection and take my personal worldviews, assumptions and biases into account during data collection and data analysis. The research design chapter will provide additional information about my role as a researcher and ethical considerations.

1.6 Thesis structure

As shown in Figure 2, the presentation of this study follows the traditional structure of a doctoral thesis and takes the form of seven chapters, including this introductory chapter.

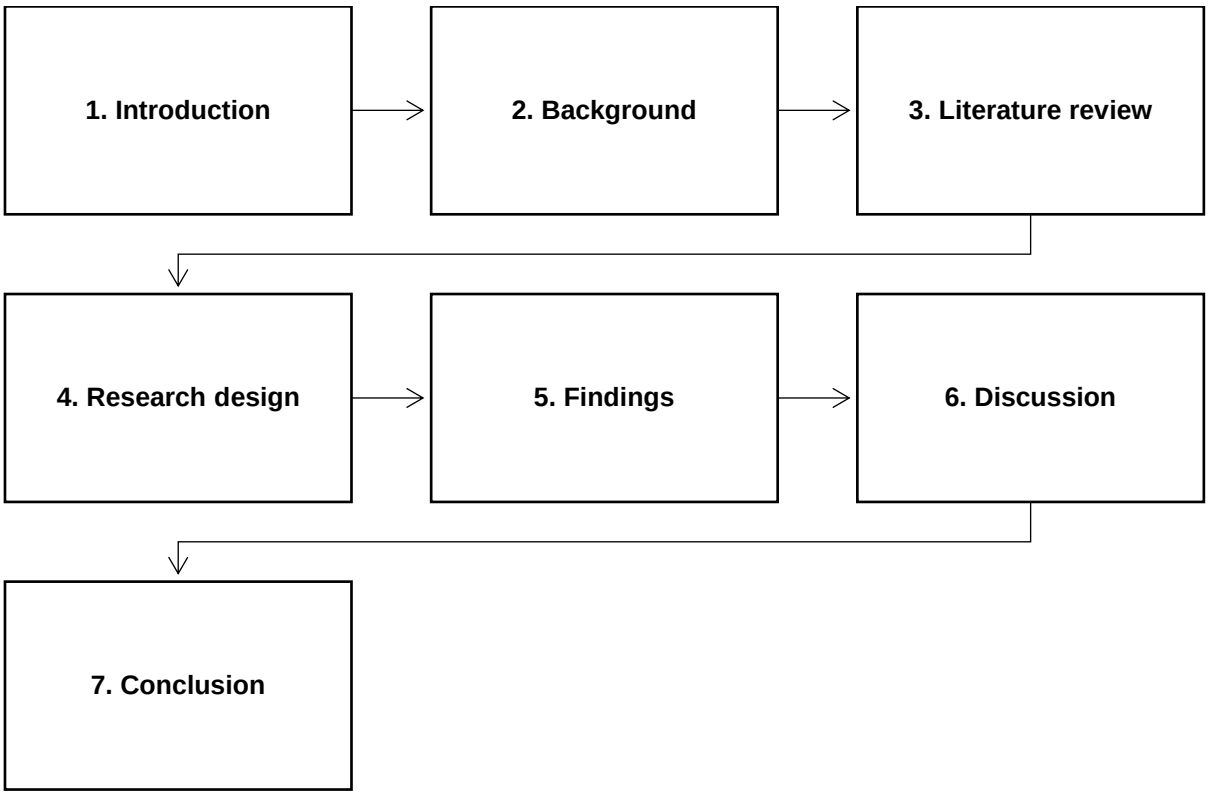


Figure 2: Thesis structure

Chapter 2 gives some relevant background information on the topic of this research. This includes the basic concepts and current state in cloud computing, the impact of the global surveillance disclosures on cloud computing services and the trust issues involved.

Chapter 3 reviews the body of literature relevant to the objectives of this research. Key aspects of the review are the definition of the concept of trust and the different trust relationships in buyer-seller trust.

Chapter 4 is concerned with the research design used for this study. This includes the research paradigm, research methodology, research method, data collection and analysis.

Chapter 5 presents the findings of the current research, focusing on the key themes that emerged from the data.

Chapter 6 discusses the findings in relation to the existing scholarly and professional literature. The chapter is structured according to the objectives of this research.

Chapter 7 draws upon the entire thesis, tying up the various theoretical and empirical strands. Key elements of this chapter are the contribution of this research to knowledge and practice. The last section discusses the limitations of this study and gives recommendations for future research.

2 Background

This chapter of the thesis gives some relevant background information on the topic of this research and is divided into four sections (see Figure 3). The first section of this chapter will define the basic terminology and concepts of cloud computing and give an overview of the importance of cloud computing services for businesses. This section will also discuss the roles of U.S. cloud providers and German cloud consumers and the concerns of German companies of public cloud services.

The following section will focus on the global surveillance activities of the U.S. intelligence agencies and is divided into two parts: the events before the disclosures by Edward Snowden and the time after the revelations. The main focus in this section is on the impact of the global surveillance disclosures on the cloud computing business in Germany.

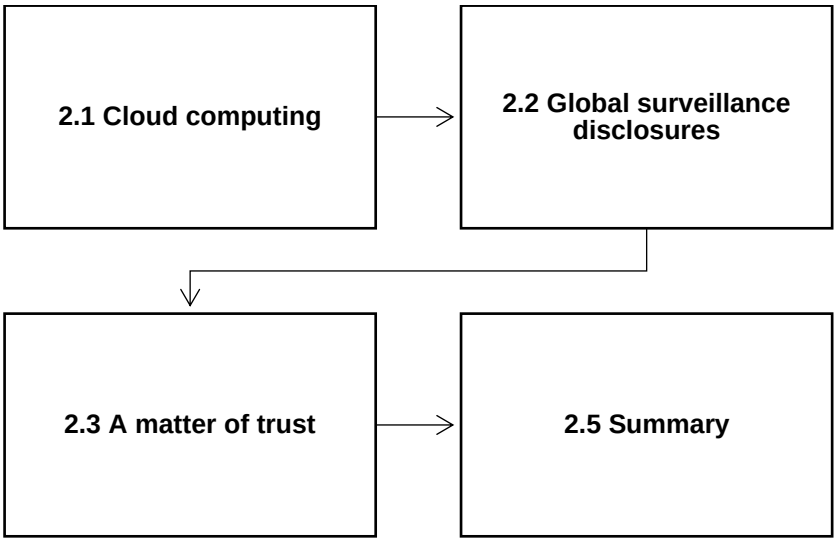


Figure 3: Background chapter

Section 2.3 will highlight how the global surveillance disclosures changed the trust of German citizens and companies in the U.S. government and U.S. cloud providers. Additionally, it will show the responses of cloud providers in the U.S. and in Germany to the changed market conditions. The last section will summarise the background information provided in this chapter and lead over to the following literature review.

Since the global adoption of cloud computing technologies is a relatively new phenomenon, parts of this chapter are based on practitioner literature and surveys from private research companies. This is also the case for the literature on the global

surveillance disclosures presented in this chapter, where academic studies were not available. The inclusion of practitioner literature allows for a more current and more detailed discourse on these recent topics. The literature review chapter, on the other hand, will primarily focus on scholarly studies and address the gaps in the current academic literature.

2.1 Cloud computing

The invention of the Internet had a profound impact on all facets of people's lives (Colley & Maltby, 2008). Since the 1990s, the worldwide use of the Internet has exploded and about 46% of the world population are now Internet users (Internet Live Stats, 2016). The potential of cloud computing services generally grows in parallel with the advancements in Internet technologies, and as the Internet grows, so does cloud computing (Erl, Puttini, & Mahmood, 2013). The changes experienced by the introduction of cloud computing over the past decade remain unprecedented.

The IT research firm Gartner predicts that, by 2020, worldwide public cloud services market revenue will reach $411B and that about one third of all IT spending will be for cloud-based infrastructure, middleware, application and business process services (Gartner, 2017). They concluded that this would make cloud computing “one of the most disruptive forces of IT spending since the early days of the digital age” (Gartner, 2016, p. 1). Market analysts IDC also expects high annual growth rates of cloud computing usage (IDC, 2012, 2013a, 2013b, 2013c, 2014, 2015, 2016, 2017).

Although cloud computing is a relatively new IT and business model, it could be argued that it is rather a new name for an old idea of computing as a utility (Armbrust et al., 2010; Michael, 2009; Weinhardt et al., 2009). The concepts behind cloud computing can be attributed to John McCarty, who already in 1961 predicted that “computing may someday be organized as a public utility” and that the “computer utility could become the basis of a new and important industry” (Garfinkel & Abelson, 1999, p. 1). Parkhill (1966) pictured the same idea and described already at that time the characteristics of modern cloud computing such as the impression of unlimited supply. As argued by Garfinkel (2011, p. 2), fifty years later this idea starts to make “financial sense” and the economies of scale could be “mind-blowing”. Arthur (2010) claimed that, the same way as firms and factories have replaced individual power generators with centrally provided electricity, companies could abandon large parts of their data centres in

favour of cloud computing services. Cloud computing can also be thought of as an evolution of IT outsourcing (Pearson, 2012), utility computing, cluster computing and grid computing (I. Foster, Zhao, Raicu, & Lu, 2008). Prominent examples of early enterprise cloud services are Salesforce.com, founded in 1999, Amazon Web Services (AWS) launched in 2002, Google Apps from 2006 and Microsoft Azure from 2010 (Erl et al., 2013).

The rapid growth and disruptive potential on traditional and new businesses make cloud computing an important subject for business research. Before proceeding to examine the business benefits of public cloud computing, it will be necessary to define what cloud computing is and to have a common understanding on the basic concepts of cloud computing technologies.

2.1.1 Terminology

The term cloud computing was defined in many different ways (Armbrust et al., 2010; I. Foster et al., 2008; Gartner, 2008) and, as pointed out by Marston, Li, Bandyopadhyay, Zhang, and Ghalsasi (2011, p. 177), there were “perhaps as many definitions as there are commentators on the subject”. Vaquero, Rodero-Merino, Caceres, and Lindner (2008) have studied over 20 definitions from academic and practitioner sources and concluded that there was no clear and complete definition of cloud computing in the literature. Gartner (2009, p. 1), one of the world's leading information technology research companies, described cloud computing as “a style of computing in which scalable and elastic IT-enabled capabilities are delivered as a service to external customers using Internet technologies”. The global research firm Forrester (2013, p. 1) defined cloud computing as “a standardized IT capability (services, software, or infrastructure) delivered in a pay-per-use, self-service way” and argued that they did not need “more or better definitions” of cloud computing (Staten, 2009, p. 1).

Technology companies, such as Amazon (Varia, 2008), Cisco (2009), Citrix (2012), HP (2011), IBM (2010) and Microsoft (2010) have all created their own definition of cloud computing. However, most of those companies are also members of the Cloud Computing Work Group (OpenGroup, 2013), which based its definition of cloud computing on the publications of the U.S. National Institute of Standards and

Technology (NIST). In October 2011, after two years in the works, the NIST published the following definition of cloud computing:

> *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. (NIST, 2011b, p. 2)*

Despite some critics (McKendrick, 2012), "The NIST Definition of Cloud Computing" received industry-wide acceptance (Erl et al., 2013; OpenGroup, 2013) and several publications on cloud computing started to apply this definition (Armbrust et al., 2010; Arora, Biyani, & Dave, 2011; CSA, 2011; C. Harding, 2011; Marinescu, 2017; Pearson, 2012; Vacca, 2016; Wang, Ranjan, Chen, & Benatallah, 2017). The NIST definition was also adopted by the European Network and Information Security Agency (ENISA, 2013) and the German Federal Office for Information Security (BSI, 2013). However, a note to the definition says that "cloud computing is (still) an evolving paradigm" and that the definition is intended to "provide a baseline for discussion from what is cloud computing to how to best use cloud computing" (NIST, 2011b, p. 1).

Since German government agencies, EU bodies, the U.S. government, most of the largest cloud providers and numerous academic papers are referring to the NIST definition of cloud computing, this study will also utilize the definitions of the NIST for the cloud computing characteristics, service models and deployment models. Regarding the current research, this definition clearly distinguishes public cloud services from traditional on-premise data centres, traditional outsourcing offerings and private cloud setups that do not comply with the NIST specification. This distinction is important for the interview process and analysis of the respondents' statements.

People and organisations can assume different roles in a cloud computing environment, depending on how they interact with or are related to it (Erl et al., 2013). As listed in Table 1, the NIST cloud computing reference architecture defines five major roles, which are cloud consumer, cloud provider, cloud auditor, cloud broker and cloud carrier (F. Liu et al., 2011).

Table 1: Cloud computing roles. Adapted from F. Liu et al. (2011, p. 4).

Role/Actor	Definition
Cloud consumer	A person or organization that maintains a business relationship with, and uses service from, cloud providers.
Cloud provider	A person, organization, or entity responsible for making a service available to interested parties.
Cloud auditor	A party that can conduct independent assessment of cloud services, information system operations, performance and security of the cloud implementation.
Cloud broker	An entity that manages the use, performance and delivery of cloud services, and negotiates relationships between cloud providers and cloud consumers.
Cloud carrier	An intermediary that provides connectivity and transport of cloud services from cloud providers to cloud consumers.

The most important roles for the current study are the cloud consumer and the cloud provider, representing the buyer and the seller in a buyer-seller relationship. A cloud consumer is an organisation or a person that has a formal contract with a cloud provider to use IT resources that are hosted by the cloud provider (Erl et al., 2013). As shown in Figure 4, the cloud consumer uses a cloud service consumer, which is a temporary runtime role of a software program, to connect to a cloud service (Erl et al., 2013). A cloud provider is responsible for maintaining the cloud infrastructure and making a cloud service available to a cloud consumer as defined in the SLA between the two parties (Erl et al., 2013).

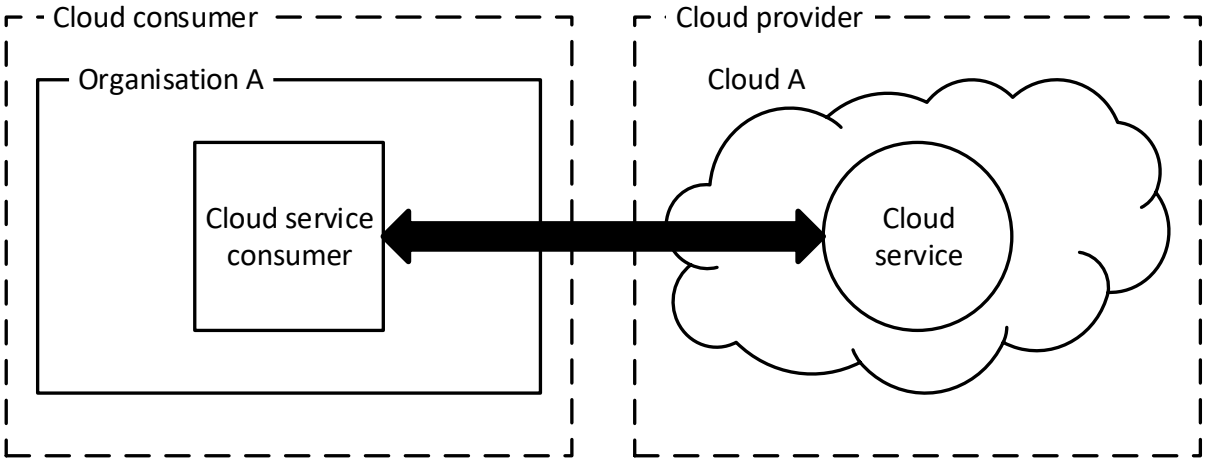


Figure 4: Cloud consumer and provider relationship. Adapted from Erl et al. (2013, p. 52).

Having defined what is meant by cloud computing and cloud computing roles, it is necessary to define some basic concepts of cloud computing.

2.1.2 Basic concepts

Before proceeding to examine the potential benefits of public cloud computing for businesses, it is important to understand how this approach distinguishes from other deployment models. Furthermore, it is necessary to create a mutual understanding of the essential characteristics of cloud computing and the cloud computing service levels discussed in this research.

As shown in Figure 5, the NIST (2011b) cloud model is composed of five essential characteristics, three service models, and four deployment models.

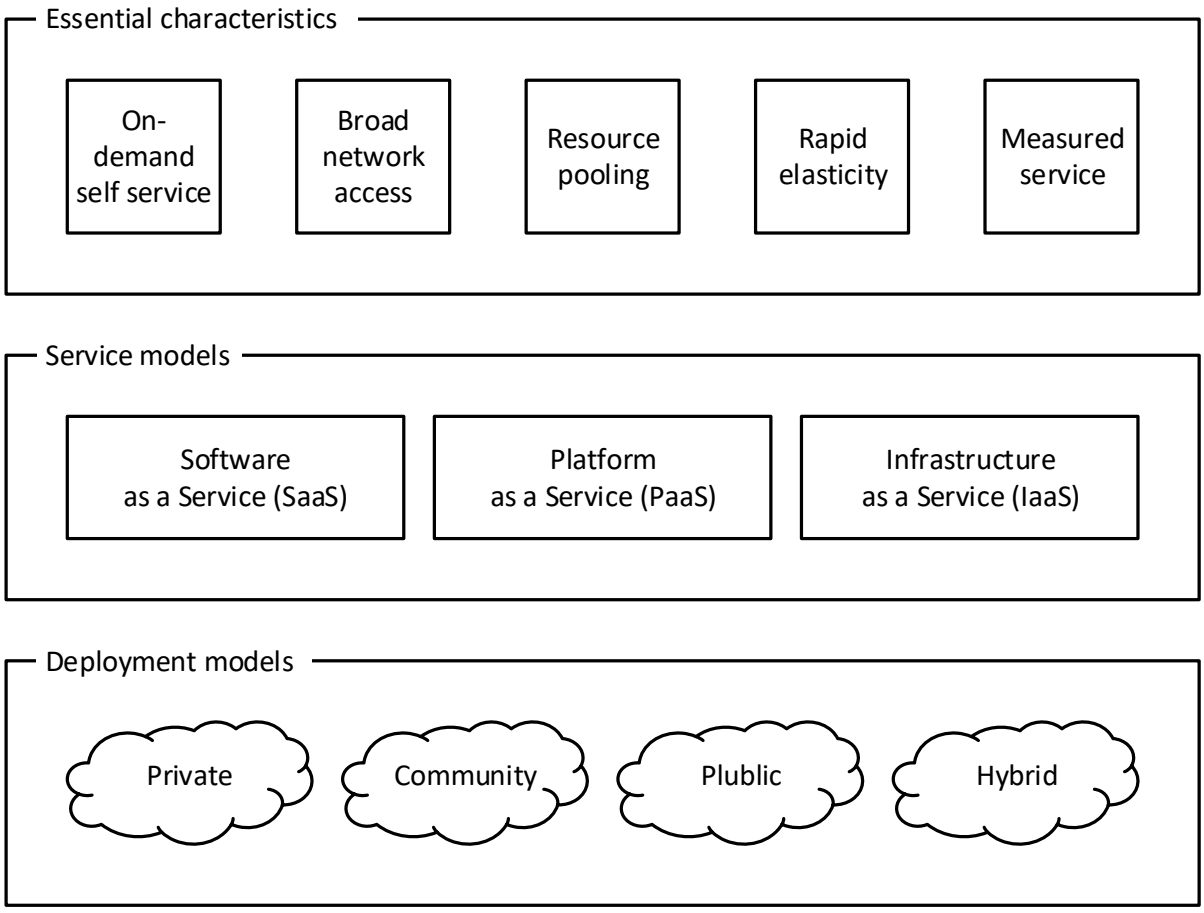


Figure 5: Cloud essential characteristics, service models and deployment models

The first basic concept are the essential characteristics of cloud computing. A cloud computing infrastructure requires a definite set of characteristics to enable the remote provisioning of scalable and measured IT resources to a meaningful extend (Erl et al., 2013). As can be seen in Table 2, the NIST (2011b) defines the following five essential characteristics: on-demand self service, broad network access, resource pooling, rapid elasticity and measured service.

Table 2: Essential cloud computing characteristics. Adapted from NIST (2011b).

Characteristic	Definition
On-demand self-service	A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
Broad network access	Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick 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 a sense of location independence in 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 data centre). Examples of resources include storage, processing, memory, and network bandwidth.
Rapid elasticity	Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
Measured service	Cloud systems automatically control and optimize resource use 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 the provider and consumer of the utilized service.

Cloud computing environments which do not meet those requirements are therefore not considered a cloud infrastructure as defined by the NIST. For example, a virtualised server farm in a private data centre of a company is not a private cloud if it does not meet the five characteristics defined by the NIST. A sixth common characteristic of cloud computing, which was not defined by the NIST (2011b), is resiliency. With resilient computing, cloud providers can increase both availability and reliability by distributing redundant implementations of IT resources across different physical locations within the same cloud or even across multiple clouds (Erl et al., 2013).

The second basic concept is the cloud computing services models. A service model, also known as delivery model, is a pre-packaged combination of specific IT resources that are offered by a cloud provider (Erl et al., 2013). As can be seen in Table 3, the NIST (2011b) defined the following three core cloud computing service models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS).

Table 3: Cloud computing service models. Adapted from (NIST, 2011b, p. 2).

Service model	Definition
Software as a Service (SaaS)	The capability provided to the consumer is to 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. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities.
Platform as a Service (PaaS)	The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created 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 deployed applications; and possibly limited control of select networking components (e.g. host firewalls).

Next to these three common service models, many specialized variations have emerged (Erl et al., 2013; Pearson, 2012; Tassabehji & Hackney, 2016). These include Security as a Service, Testing as a Service, Communications as a Service and Storage as a Service. Figure 6 compares the three main services models to traditional IT service models and shows the responsibility for managing each IT resource.

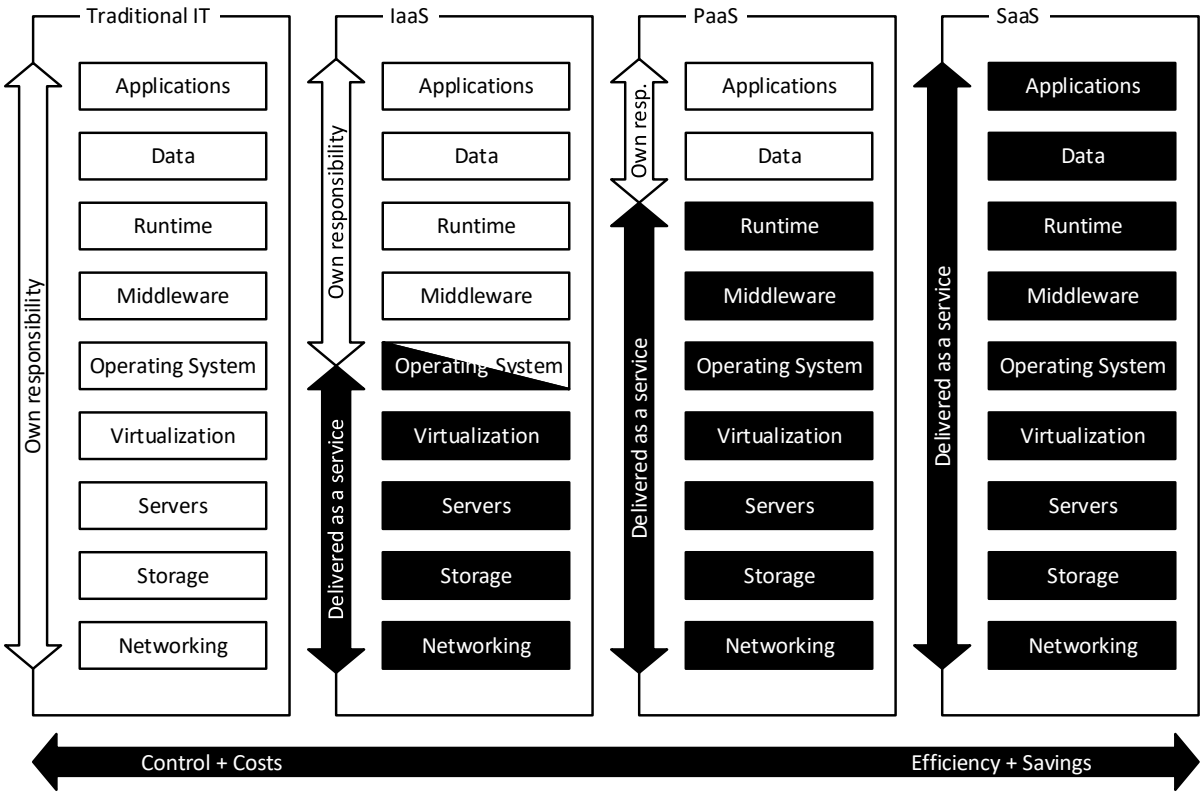


Figure 6: Cloud computing service models. Adapted from Harms and Yamartino (2010).

An IT resource is a physical or virtual IT-related artefact which can be hardware-based, e.g. a network device, or software-based, e.g. a virtual server (Erl et al., 2013). The more IT resources are delivered "as a service", the lower are the costs for the cloud consumer because those IT resources are designed to run in a cloud environment and are managed by a cloud provider who can take advantage of the economies of scale in the cloud (Harms & Yamartino, 2010). Consequently, companies need to invest time and resources to tailor the cloud computing service models to the individual context and service requirements of their organisation (Tassabehji & Hackney, 2016).

The current study did not focus on any specific service model but included all three options. However, several interviewees referred to these models when describing their cloud computing ambitions and the interviewees from the U.S. cloud providers were selling different combinations of cloud computing service models.

The third basic concept is the cloud computing deployment model, which characterises a particular type of cloud computing environment that can be distinguished by ownership, size and access (Erl et al., 2013). As explained in the following section, this study primarily focused on the public cloud deployment model. However, it is

important to understand the differences between the four most common cloud computing deployment models (private cloud, community cloud, public cloud and hybrid cloud), which are summarised in Table 4.

Table 4: Cloud computing deployment models. Adapted from (NIST, 2011b, p. 3).

Deployment model	Definition
Private cloud	The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g. business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
Community cloud	The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g. mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.
Public cloud	The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.
Hybrid cloud	The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g. cloud bursting for load balancing between clouds).

In addition to these four basic cloud computing deployment models, other variations, such as virtual private clouds, partner clouds and inter-clouds can exist (Erl et al., 2013; Millard, 2013; Pearson, 2012). As was pointed out in this section, the current study focused on the public cloud deployment model. In the following section, it will be argued that public cloud computing offers the most benefits for businesses in terms of cost reduction and operational benefits. Throughout this thesis, the term cloud provider will be used to refer to public cloud service providers.

2.1.3 Business benefits of public cloud computing

Cloud computing provides enormous potential for efficiency and new business opportunities by transforming current information technology infrastructures, models and services (Antonopoulos & Gillam, 2017; Ruparelia, 2016; Wang et al., 2017). Today, cloud computing already creates significant value for companies by making information technology more efficient, more powerful, simpler and faster (Faynberg, Lu, & Skuler, 2016; MGI, 2013) and most business and IT executives believe that cloud computing is delivering efficiencies and cost savings today (KPMG, 2013; Wang et al., 2017). According to the European Commission (2012d, p. 4), “substantial

efficiency improvements across the whole economy can be expected from cloud adoption by businesses and other organisations".

Companies worldwide are moving their on-premise IT to cloud computing deployment models, and of these models described in Section 2.1.2, public cloud computing offers the most business advantages (Domnik, 2015; KPMG, 2012). Obeidat and Turgay (2013, p. 174) argued that "the adoption of cloud computing leads to a balance of benefits over costs" and that "managers should ensure that their organizations adopt cloud computing technology" (Obeidat & Turgay, 2013, p. 174). The following is a summary of the primary business advantages of the public cloud deployment model.

Cost savings

One of the key business drivers for public cloud computing adoption is cost savings (Avram, 2014; European Commission, 2012d; C. Harding, 2011; NIST, 2011a; Rittinghouse & Ransome, 2017). IT capital expenditure can account for about half of the total annual IT budget of a company. By moving to a public cloud solution, companies can shift their capital expenses (CAPEX) to operating expenses (OPEX) and thereby achieve significant cost savings (Andrikopoulos, Binz, Leymann, & Strauch, 2013; CEBR, 2010; Faynberg et al., 2016). The on-demand self-service and measured service characteristic of cloud computing (see Section 2.1.2), and the pay-as-you-go principle of the public cloud deployment model (Erl et al., 2013; Wang et al., 2017), result in a considerably higher cash flow for companies (C. Harding, 2011; Ruparelia, 2016). The released capital can thereupon be invested in the core business of a company. Large cloud providers have more standardized system architectures and their buying power allows them to buy hardware at up to 30% lower prices than smaller buyers (Harms & Yamartino, 2010; Jamsa, 2012).

Furthermore, the shift from CAPEX to OPEX decreases the overall capital investment risks of organisations (Pearson, 2012; Rittinghouse & Ransome, 2017). Operational costs represent another large share of the IT budget of a company which often exceeds the up-front infrastructure investment costs (Antonopoulos & Gillam, 2017; Erl et al., 2013). Examples for operational costs are personnel expenses, trainings, security measures, software licensing, hardware repairs, third party support, building costs, cooling and power supply (Andrikopoulos et al., 2013; Erl et al., 2013; Ruparelia, 2016; Wang et al., 2017). Electricity costs have become the largest part of the total

cost of ownership (TCO) of enterprises data centres (Harms & Yamartino, 2010; Ruparelia, 2016) and while the owners of small or medium sized data centres have to pay the local rates for electricity, large cloud providers can negotiate bulk purchase agreements and build their server farms in places where power is comparatively cheap (Antonopoulos & Gillam, 2017; Arora et al., 2011).

The economies of scale of public cloud computing also have an impact on labour costs (CEBR, 2010; Ruparelia, 2016). In a traditional enterprise data centre, a system administrator can take care of about 140 servers, whereas in a cloud data centre the same person can manage thousands of servers (Harms & Yamartino, 2010). Additionally, traditional data centres are designed for peak usage scenarios and the available capacity of the servers is unused most of the time (Arora et al., 2011; Ruparelia, 2016).

A key economic advantage of public cloud computing is also the capability to address fluctuations in resource utilisation by pooling IT resources (see Section 2.1.2) and workloads from a large number of customers with different work practices (random variability), from different time zones (time-of-day patterns), from different sectors (industry-specific variability), with various applications (multisource variability) and with individual needs for scalability (uncertain growth patterns) (Harms & Yamartino, 2010; Wang et al., 2017). Consequently, by pooling IT resources and workloads, public cloud providers can avoid server idle times and optimise data centre utilisation and infrastructure investments (Antonopoulos & Gillam, 2017).

Agility

Another key reason for public cloud computing is agility (C. Harding, 2011; Ruparelia, 2016; Wang et al., 2017). Organisations need to be able to respond to internal and external factors by scaling their IT resources in relation to current business requirements (Erl et al., 2013). The rapid elasticity and on-demand self-service characteristics of cloud architectures (see Section 2.1.2) provide companies with real-time access to high performance computing with almost unlimited scalability (Arora et al., 2011; Rittinghouse & Ransome, 2017). The increase and decrease of IT resources can be configured fully automatically without human intervention and because of the measured service characteristic described in Section 2.1.2, companies only pay for the IT resources they actually utilise (C. Harding, 2011; Wang et al., 2017).

Furthermore, because cloud architectures can scale out almost instantaneously, companies can considerably reduce the time to market period for new products and services (Wang et al., 2017). With public cloud computing, hardware resources can be provisioned within minutes or hours versus days or weeks with traditional data centres. With public cloud computing, companies do not need to procure and install new hardware but have the ability to almost instantaneously run different workloads in parallel in the cloud (Antonopoulos & Gillam, 2017; Arora et al., 2011).

Not only large enterprises and SMEs benefit from the agile characteristics of cloud computing, also entrepreneurs and start-up companies have the ability to create business models that have not been possible in the past (R. Smith, 2009; Wang et al., 2017). The “elasticity” characteristic of cloud computing allows them to grow their businesses at any pace they like and transparently scale IT resources with no or reduced investment costs (Erl et al., 2013). Cloud computing therefore raises the incentives for new business creation and encourages entry into and increases competition in old and new markets (CEBR, 2011; Wang et al., 2017).

Productivity

The third main reason for using public cloud computing is increased productivity. The use of cloud-based services for instant messaging, email, file sharing, voice and video communication, calendaring and document creation is becoming a common way of working in many companies (C. Harding, 2011; Ruparelia, 2016). This also includes the mobile access to these applications with smartphones, tablets and laptops (Antonopoulos & Gillam, 2017).

Availability

Another business benefit is a higher availability of business-critical applications (Wang et al., 2017). Business needs may require certain IT services to be more reliable (Bhowmik, 2017; Erl et al., 2013). High availability with geographically distributed data centres is a default setup with many public cloud providers (Arora et al., 2011; Rittinghouse & Ransome, 2017) and the guaranteed “uptime” is usually specified in a service level agreement (C. Harding, 2011; Wang et al., 2017). Public cloud providers are able to patch servers and platforms and upgrade applications without service interruption (Arora et al., 2011; Dempsey & Kelliher, 2017). Therefore, public cloud

providers can achieve a much higher level of service availability than companies can realise with their own traditional data centres (Rittinghouse & Ransome, 2017).

Nevertheless, not all cloud providers are able to offer the same level of features, performance, reliability and prices. As argued in the next section, U.S. public cloud providers are dominating the cloud market and their solutions are in most cases superior to those from European or German providers.

2.1.4 U.S. cloud provider

Today, the most advanced public cloud computing solutions are offered by U.S. cloud providers (Büst, 2016; Castro, 2013; Experton, 2012; Herrmann, 2017; Millard, 2013; Schechner, 2016). U.S. companies such as Amazon, Google, Microsoft and Salesforce have pioneered many cloud computing technologies. Today, these companies are the most important, best known and most frequently mentioned cloud providers in the German market (Böken, 2011; Deloitte, 2011; Herrmann, 2017). Even many German cloud providers are building their SaaS services on top of IaaS solutions of U.S. cloud providers or re-selling U.S. cloud solutions (Böken, 2011; T-Systems, 2017). The Cloud Vendor Benchmark 2014 for the German market by Experton (2014) also showed that the market leader quadrants for all three cloud computing services models (IaaS, PaaS and SaaS) were dominated by U.S. companies. The European Commission (2015b, p. 76) concluded that the public cloud market in Europe was "dominated by U.S. vendors and though there are strong and innovative public cloud providers in Europe, this dominance will continue, though it may lessen to some degree over time as the market matures". As shown in Table 5, nine out of the top ten cloud providers in the European market were headquartered in the U.S. with SAP as the only European provider.

Table 5: Top 10 cloud providers in Europe. Adapted from European Commission (2015b).

Top 10	Name	Revenues (€m)
1	Salesforce	885.92
2	Amazon	771.89
3	Microsoft	354.21
4	Google	302.52
5	Oracle	259.58
6	IBM	256.60
7	Adobe	224.98
8	SAP	214.34
9	Symantec	204.71
10	GXS (OpenText)	179.07

According to Experton (2012), one of the key reasons why German cloud providers did not grow in the same pace as U.S. cloud providers was a lack of qualified staff. Likewise, the European Commission (2015b, p. 76) suggested that the availability of skilled staff gives U.S. vendors an advantage over European vendors. Another reason for the dominance of U.S. cloud providers could be that they had a “first-mover advantage” (TNW, 2016). For example, Amazon Web Services was created as an internal IT service provider for the retail business of Amazon and became the world’s largest IaaS cloud provider (Hern, 2017). It might therefore be difficult for German or EU cloud providers to reach similar economies of scale with a competitive pricing model. Likewise, in a study mandated by the European Commission (2015b, p. 12), the authors also argued that the U.S. cloud providers had an “early mover advantage” and that European cloud providers had to be successful in multiple countries in order to “get close to the opportunity that exists in the U.S.”. Other reasons named in the study were the complex legal frameworks in Europe and the lack of a common language.

Storing or processing data in data centres in the U.S. or in data centres owned by U.S. cloud providers causes several challenges to German companies. The following sections will give an overview of the German cloud market and those challenges.

2.1.5 German cloud consumer

In comparison with their neighbours in Europe or with other developed countries, German companies have a relatively low adoption rate of public cloud computing services (Nikoloff, 2013). According to data from a publication issued by Eurostat (2017), the statistical office of the European Union, only 16% of all enterprises in Germany used cloud computing services, which was one of the lowest adoption rates in the EU28 member states (see Figure 7). The EU28 average was 21%, the UK had an adoption rate of 35%, and 57% of the companies in Finland used cloud services.

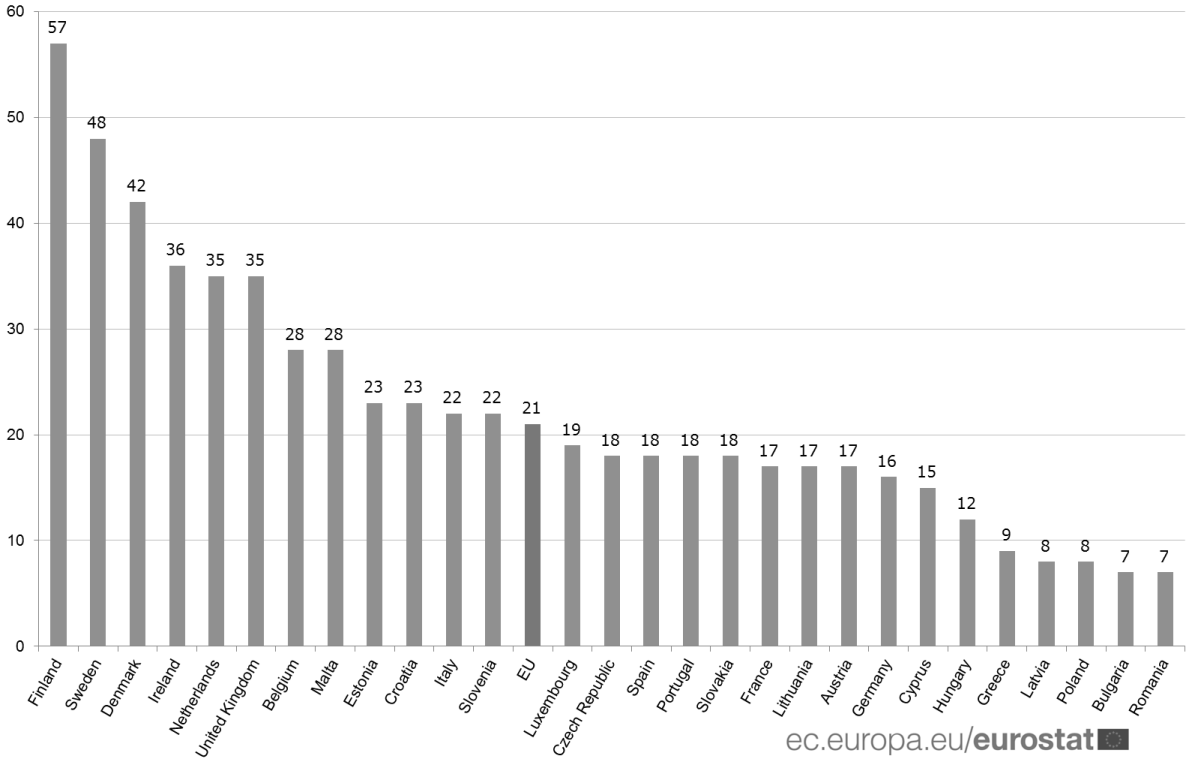


Figure 7: Use of cloud computing services in the EU. Adapted from Eurostat (2017).

An international survey conducted by NTT (2014) with 1,000 IT decision makers from France, Germany, Hong Kong, UK and USA revealed that Germany had the lowest average cloud usage. Likewise, in a recent study with 2,600 SMEs in Belgium, France, Germany, the Netherlands, Spain, UK and the USA, German companies had the lowest cloud adoption of all countries (Exact, 2016).

In Germany, in distinction to many other countries, small and medium enterprises (SMEs), the so called Mittelstand, accounts for 35% of the total revenue of all German companies and are therefore a very important part of the country's economy (IfM, 2015). While cloud computing provides many opportunities for German businesses, the German SMEs would benefit most from the capabilities of cloud computing technologies (BDO, 2014; Holtkamp, 2010; Microsoft, 2013; PwC, 2011; Trigueros-Preciado, Pérez-González, & Solana-González, 2013). According to BITKOM, Germany's largest information and communication technology association, especially SMEs could reach higher security standards through public cloud computing than with their own local IT (Kerkmann, 2013b). SMEs often do not have the needed resources and know-how or cannot achieve the necessary economies of scale in a way that large enterprises can (Goyal, 2014; IDC, 2012). Public cloud computing gives SMEs access

to powerful IT infrastructure and software without the need to actually buy them (Erl et al., 2013; IDC, 2013a). The pay-per-use model of public cloud computing allows SMEs to avoid large up-front IT investments, namely hardware and software ownership cost, and gives them the opportunity to compete with larger enterprises without having to spend their money on IT infrastructure (CEBR, 2011; Experton, 2012; Rittinghouse & Ransome, 2017). However, the cloud adoption rate of SMEs in Germany is even lower than the adoption by large companies (KPMG, 2015).

Another important aspect is the sector or industry a company is operating in. According to a study conducted by Techconsult (2012), the cloud computing usage in Germany was relatively similar between different sectors or industries (see Figure 8). With a usage rate of 20%, the public sector had the lowest adoption rate in Germany, whereas the trade sector had the highest rated with 29%.

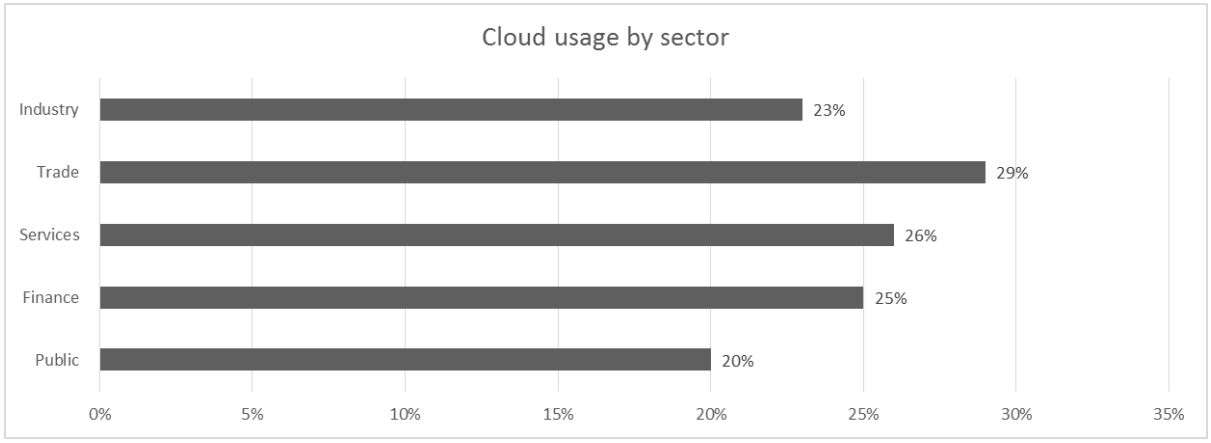


Figure 8: Cloud usage by sector. Adapted from Techconsult (2012)

Based on these figures, the current research was designed to be sector-independent and did not take the characteristics of each individual industry into consideration. However, as it will be detailed in the findings and discussion chapters, this assumption turned out to be incorrect for the companies of the current research. Consequently, this connection between sectors and cloud adoption was emphasised in the discussion chapter and also needs to be addressed in future research.

The overall low percentage of cloud usage in Germany can have several reasons. The following sections will provide some background information on two aspects of the German society and economy that were repeatedly mentioned by the interviewees.

2.1.5.1 German history and culture

Throughout the public discussions about the trust of German citizens and corporations in the U.S. government and U.S. cloud services, several academics and politicians highlighted a possible distinctiveness of the German society because of the German history and culture (Birnbaum, 2013; Curry, 2015; Dearden, 2014; M. Fisher, 2013; Hovenstädt, 2013; Kirschbaum, 2014; Noack, 2015; Zaske, 2015).

The authors reasoned that the tolerance of mass surveillance programmes was much lower in Germany than in other countries because of the German history of “Nazism and East Germany's Stasi secret police” (Bryant, 2013b, p. 1). They argued that the German history of dictatorship made the citizens “particularly sensitive to violations of personal privacy” (Karnitschnig, 2014, p. 2).

In January 2014, in his public speech on the NSA mass surveillance activities, U.S. President Barack Obama (2014, p. 1) cited the example of the Stasi in East Germany as “a cautionary tale of what could happen when vast, unchecked surveillance turned citizens into informers, and persecuted people for what they said in the privacy of their own homes”. In an interview he gave some months later, Obama acknowledged that “there are some countries like Germany, given its history with the Stasi, that are very sensitive to these issues”. (Swisher, 2015, p. 10). German Chancellor Angela Merkel, however, stated that there was “absolutely no comparison between the Stasi in East Germany and the work of intelligence services in democratic states”. In her opinion, these were "two totally different things, and such comparisons only led to a trivialization of what the Stasi did to the people in East Germany" (Spiegel Online, 2013, p. 1).

The current literature on the relationship between culture and trust, cultural differences between the U.S. and Germany and culture models in organisational research will be reviewed in Chapter 3. Furthermore, the German history and cultural differences between the U.S. and Germany and the impact on cloud computing adoption will be examined in more detail in the findings and discussion chapters.

A major concern regarding public cloud computing which was also addressed during the interviews for this research is about economic espionage. The next section will therefore give some background information on the relationship between cloud computing and the fear of economic espionage in Germany.

2.1.5.2 Economic espionage

The German economy is particularly dependent on exports of high-tech products such as machinery and chemistry which means that the protection of intellectual property and patents are of constant concern for German companies (Bryant, 2013b; Destatis, 2017). Many German SMEs are market leaders in their particular niche but lack the financial resources and personnel to protect themselves from intellectual property theft (Bryant, 2013c). The German engineering association VDMA, one of the largest industrial associations in Europe, worried that these so called “hidden champions” of the German economy were a major target for economic espionage by U.S. intelligence agencies (Mortsiefer, 2013). Those companies fear that if they store their confidential company data at a U.S. cloud provider, the U.S. government would have access to this data and could potentially support their own economy by passing this information secretly to U.S. companies. This data may contain construction plans, patent applications, merger and acquisition strategies or other confidential material.

In a survey conducted by Ernst & Young in 2013 with over 400 German companies, about 26% of German IT managers described the U.S. as a high risk for data theft and economic espionage (EY, 2013). This was the second place after China (28%) and before Russia (12%). In a similar survey that Ernst & Young conducted two years earlier, before the revelations of the global surveillance disclosures (see Section 2.2), only 6% of the respondents named the U.S. as a major threat. However, not only German companies see economic espionage as a major challenge for cloud adoption. In a survey by KPMG in 16 countries, the respondents named the risk of intellectual property theft as the most challenging area of all security issues (KPMG, 2013).

This view is also shared by official representatives of the German economy. Ulrich Brehmer, board member of the German Association for Security in Industry and Commerce (ASW), which is the central organization of the German economy for security matters, stated that foreign intelligence agencies often have the mandate to strengthen the domestic economy (Zacharakis, 2013). He added that there is a risk that the data collected by U.S. intelligence agencies is used for economic espionage of German companies (K. Bode, 2013) and that his organisation does not know what exactly happens with the collected data (Obermaier & Schultz, 2013). Brehmer was also worried about the fact that the U.S. intelligence agencies are working with private

consulting companies and that these consultants may sell collected information to other companies (Brauck et al., 2013). The president of the Federation of German Industries (BDI), Ulrich Grillo, stated that economic espionage by U.S. intelligence agencies on German companies was not acceptable and constitutes a violation of international law (Dieckmann, 2013). He warned that lost trust would have fatal consequences for the business relationships between the U.S. and Germany (Spiegel Online, 2015a). In April 2016, the German Domestic Intelligence Service (BfV) launched together with industry associations the "Economic Security Initiative" to "jointly develop and implement measures to improve economic security" (BfV, 2017, p. 34).

The discussion about economic espionage on German companies was fuelled by an interview with the former NSA contractor Edward Snowden who told Germany's largest public broadcaster ARD that U.S. intelligence agencies would spy on large German enterprises that compete with U.S. companies (BBC, 2014b; Kirschbaum, 2014). He stated that "there's no question that the U.S. is engaged in economic spying" and that "if there's information at Siemens that they think would be beneficial to the national interests, not the national security of the United States, they'll go after that information and they'll take it" (NDR, 2014, p. 4).

A representative of the U.S. government rejected the accusations made by Edward Snowden. The chairman of the House Intelligence Committee, Mike Rogers, stated that the claims that the NSA would spy for the competitive advantage of the U.S. industry were wholly untrue. He said that "economic espionage is against the law in the United States. If they [the NSA] do it, they are going to jail. Period." (Sam Jones, 2014, p. 1).

However, the topic of economic espionage by the U.S. intelligence agencies remains a concern among German businesses (Spiegel Online, 2015b) and was also one of the key topics addressed by the interviewees of this research.

2.1.6 Concerns about public cloud computing

The economic potential of cloud computing and its ability to accelerate growth and innovation are putting a lot of pressure on companies and governments to adopt cloud computing solutions (Pearson, 2012). However, the adoption of cloud computing

causes various risks, obstacles and concerns for cloud consumers (Armbrust et al., 2010; Dutta, Peng, & Choudhary, 2013; Géczy, Izumi, & Hasida, 2011; Latif, Abbas, Assar, & Ali, 2014; Taylor, 2011). The following paragraphs will summarise these concerns on an international, European and German level.

On an international level, as presented in Table 6, the top two critical cloud computing risks that have been identified by an international group of IT professionals were "privacy" and "inconsistent data protection laws" (Dutta et al., 2013).

Table 6: Top 10 cloud computing risks. Adapted from Dutta et al. (2013).

Rank	Risk events
1	Privacy of enterprise or customer data is jeopardised in the cloud
2	Inconsistent data protection laws adopted by different countries where cloud data are generated and stored
3	Difficult for user companies to change cloud vendors even in the case of service dissatisfaction (also known as vendor lock-in)
4	User companies lack disaster recovery and contingency plans to deal with unexpected technical issues in cloud environment
5	Enterprise data re-migration difficulties at the end of the cloud contract
6	Inadequate user training/knowledge on cloud services and usage
7	Cloud applications become temporarily unavailable or out-of-service
8	Increasing hidden costs due to non-transparent operating models in the cloud
9	Denial-of-Service (DoS) attacks in the cloud environment
10	Unauthorised access to enterprise data/applications in the cloud

Another international cross-industry study conducted by El-Gazzar, Hustad, and Olsen (2016) indicated that most concerns regarding public cloud computing were related to security issues, strategic issues and legal/ethical issues. The authors concluded that the specific characteristics of public cloud services "lead to a lack of trust in this technology due to the multi-tenancy architecture, remote storage of data, and enterprises' fear of losing control over their resources" (El-Gazzar et al., 2016, p. 78).

At the European level, the responses are very similar. In a study commissioned by the European Commission (2012c) and conducted by IDC, the most frequently stated barriers for cloud computing adoption, as listed in Table 7, were legal and security concerns, as well as a lack of trust in general. In a follow-up study commissioned by the European Commission (2015b), IDC did not specifically analyse the relevance of cloud barriers in Europe but commented that the actual growth rate was lower than it expected two years earlier and that barriers on legal jurisdiction, security/privacy and data location were still existent.

Table 7: Cloud barriers in Europe. Adapted from European Commission (2012c, p. 34).

Rank	Barriers
1	Legal jurisdiction (31.7%)
2	Security & data protection (30.5%)
3	Trust (25.1%)
4	Data access and portability (24.9%)
5	Data location (23.8%)
6	Local support (22.8%)
7	Change control (22.4%)
8	Ownership of customisation (21.4%)
9	Evaluation of usefulness (18.2%)
10	Slow internet connection (18.0%)
11	Local language (17.9%)
12	Tax incentives (17.4%)

German IT and business executives also have similar concerns. As listed in Table 8, some of the largest market research and professional services networks in the world have analysed the risks, obstacles or concerns associated with public cloud computing from the point of view of German companies. The following table contains the most recent studies by these research companies on the subject of concerns, obstacles and risks. Due to a lack of academic studies on this subject, all of these surveys are practitioner studies, mostly funded by private corporations. It is therefore important to acknowledge the possibility that these studies are not entirely neutral or were commissioned to serve a certain purpose. Nevertheless, they can show a certain tendency in the market and point in a certain direction for scholarly research.

The oldest study listed in Table 8 is from Deloitte (2011) who surveyed 300 German companies between December 2010 and January 2011. KPMG (2017a) interviewed 554 German companies in 2016 in cooperation with BITKOM, the German federal association for information technology. For the study by PwC (2013a), an unknown market research institute conducted 60 interviews in January and February 2013. And 200 German companies answered the survey questions of the German IT market analysis company Techconsult (2013c).

Table 8: Top 5 concerns, obstacles and risks for German companies

Author(s) Title	Topic / question	Top 5 concerns / obstacles / risks
Deloitte (2011) Cloud Computing in Deutschland	For what reasons did you decide not to use cloud computing solutions?	1. Risk of loss of governance and control (57%) 2. Insufficient data **security** / availability (55%)

		3. Open **compliance and legal** questions (48%) 4. Doubts regarding the long-term availability (34%) 5. Risk of vendor lock-in (31%)
KPMG (2017a) Cloud-Monitor 2017 (for Germany)	Barriers to public cloud computing: To what extent do these statements apply to your company?	1. Fear of **unauthorized access** to sensitive corporate data (60%) 2. **Legal and regulatory provisions** speak against it (52%) 3. Fear of **data loss** (51%) 4. Unclear **legal** situation (50%) 5. Public cloud solutions are difficult to integrate with in-house solutions (43%)
PwC (2013a) Cloud Computing: Evolution in the Cloud	What are the most important critical success factors for your customer's satisfaction?	1. Data **privacy** and information **security** (98%) 2. Reliable service availability (97%) 3. Service performance (93%) 4. Observing compliance requirements (85%) 5. Ease of integration into IT landscape (78%)
Techconsult (2013c) IT-Cloud-Index Mittelstand Cloud-Bericht August 2013	What are the greatest obstacles for the adoption of cloud services?	1. Too many **security** risks (67%) 2. Concerns regarding loss of control over IT (60%) 3. **Legal** framework / requirements (56%) 4. Vendor lock-in (48%) 5. Missing standards and therefore high integration efforts (37%)

Even though these studies were conducted by different market analyst companies in different years between 2011 and 2017, the main concerns have not changed much over time. The top three concerns raised by German companies can be summarised as

a) cloud computing security,

b) cloud computing privacy and

c) regulations, policies and legal aspects.

The following sections will describe these three top concerns in public cloud computing services in greater detail. The terms security, privacy and legal aspects will be repeatedly used in this background chapter as well as the literature review and the findings and discussion of the current research. Therefore, it is important to have a common understanding of the terms and to give some additional contextual background information relevant to the current research.

2.1.6.1 Security

The first major concern reported by the German companies in the surveys presented above is security. A widespread perception of cloud consumers is that public cloud services are inherently less secure than traditional on-premise infrastructures which might be one of the reasons why German companies are deploying more IT services in their private cloud than in public cloud services (Bhowmik, 2017; Kaufman, 2010; KPMG, 2017a). Security concerns were also mentioned as one of the main reasons which reduces cloud computing growth (Subashini & Kavitha, 2011) and the NIST (2011a, p. 8) even classified security as “the biggest obstacle facing public cloud computing”. Since cloud computing encompasses numerous technologies such as networks, operating systems, virtualisation, databases, clustering and load balancing, securing cloud data centres is a complex undertaking (Hamlen, Kantarcioglu, Khan, & Thuraisingham, 2010; Wang et al., 2017).

However, while the concentration of data in centralised data centres presents a more attractive target for attackers, public cloud computing data centres also have more robust, scalable and cost-effective security defences than local private server rooms (Bhowmik, 2017; ENISA, 2009). Particularly SMEs can achieve greater security by using public cloud computing services compared to the know-how and budget these companies can provide in-house (Pearson, 2012; Stieninger & Nedbal, 2014). In a survey conducted by Techconsult (2013b), 45% of the SMEs in Germany stated that they have none or very limited experience with IT security. However, most of these companies still considered private cloud solutions more secure than public clouds, even if they could not provide the necessary security know-how (Techconsult, 2013b).

It could be argued that many security issues with cloud computing already existed with other computer-based sharing systems (Julisch & Hall, 2010; Roberts II & Al-Hamdani, 2011). This was also the conclusion of Chen, Paxson, and Katz (2010), who maintained that only few cloud computing security issues were fundamentally new and many of those issues already existed before in outsourcing and hosting scenarios. However, Chen et al. (2010) also found that complex multi-party configurations and the need for mutual auditability were to some degree new and fundamental to cloud computing. In a study which investigated the major security issues with cloud computing, Ertaul, Singhal, and Saldamli (2010, p. 1) reported that “security is as much

of an issue in the cloud as it is anywhere else" and that many companies were not moving to the cloud because they were not able to quantify the security risks involved.

One of the reasons for this limited ability to quantify the security risks could be that with cloud computing, details about the technology and IT infrastructure are "abstracted away from the sight of the users" (Uusitalo, Karppinen, Juhola, & Savola, 2010). It could therefore be concluded that companies need a detailed understanding of the underlying concepts of public cloud computing to make the right business decisions regarding cloud security. As will be discussed in the findings and discussion chapters, German companies might underestimate the security risks associated with hosting data in their own on-premise data centre.

Nevertheless, according to Pearson (2012), while companies mostly focus on cloud computing security, the most difficult subject to address is privacy. Security, on the other hand, "is a necessary but not a sufficient condition for privacy" and it is "one of the core privacy principles" (Pearson, 2012, p. 12). Added to the security concerns frequently raised by technical experts are growing concerns from data protection supervisors, government officials and consumers about the substantial impact of cloud computing technologies on (personal) data protection in conjunction with the required compliance with local and foreign regulations (Pearson, 2012). Consequently, concerns regarding compliance with privacy regulations might be one of the key barriers for German companies adopting U.S. cloud services. Before discussing the role of regulations, policies and legal issues, the following section will focus on the concept of privacy and the levels of privacy and data protection standards of the U.S. and Germany.

2.1.6.2 Privacy

The second key barrier cited by German companies is privacy. Privacy "differs from security in that it relates to handling mechanisms for personal information" and because it is concerned with aspects such as fairness of use, access, notice, choice, accountability and also security (Pearson, 2012, p. 13). For the current research, privacy only relates to personal information, whereas security can relate to all information. Privacy is a fundamental human right which is protected by Article 12 of the Universal Declaration of Human Rights (UDHR) of the United Nations (1948) and later by Article 8 of the European Convention on Human Rights (ECHR) of the Council

of Europe (1950) and, on a national level, by Article 10 of the Basic Law for Germany (1949) (German: Grundgesetz für die Bundesrepublik Deutschland).

Privacy is, however, described as a vague concept (Solove, 2006) which is not universally defined but is a cultural construct and therefore subjective (Martucci et al., 2012). Consequently, there can be various forms of privacy (Pearson, 2012) including central concepts such as “the right to be left alone” (Warren & Brandeis, 1890) and peoples’ “right to control, edit, manage, and delete information about themselves” (Westin, 1967). Based on the work of Warren and Brandeis (1890), Prosser (1960) distinguished between four types of harmful activities related to privacy: 1) Intrusion upon the plaintiff’s seclusion or solitude, or into his private affairs, 2) Public disclosure of embarrassing private facts about the plaintiff, 3) Publicity which places the plaintiff in a false light in the public eye and 4) Appropriation, for the defendant’s advantage, of the plaintiff’s name or like-ness. However, since Prosser (1960) only focused on tort law and did not reflect current legislation and technology changes, Solove (2006) created a new taxonomy to understand privacy violations.

According to Solove (2006) there are four basic groups of harmful activities which are 1) information collection (including surveillance and interrogation), 2) information processing (including aggregation, identification, insecurity, secondary use and exclusion), 3) information dissemination (including breach of confidentiality, disclosure, exposure, increased accessibility, blackmail, appropriation and distortion) and 4) invasion (including intrusion and decisional interference). Public cloud computing can be exposed to all of those activities and offers significant challenges for organisations that have to meet certain privacy regulations (Pearson, 2012). The global surveillance actions that will be discussed later in this chapter may have involved several of these harmful activities.

According to Miltgen and Peyrat-Guillard (2014, p. 105), many scholars define information privacy as “an individual desire to control or have influence over the acquisition and potential secondary uses of personal data”, e.g. Bélanger and Crossler (2011); Bélanger, Hiller, and Smith (2002). Information privacy and trust are closely linked concepts, though their exact relationship remains a topic of debate (Miltgen & Peyrat-Guillard, 2014). Trust can be connected to both information privacy and disclosure (Fogel & Nehmad, 2009), can mediate between them (Dinev & Hart, 2006),

can be an antecedent (Bélanger et al., 2002; Eastlick, Lotz, & Warrington, 2006) or a consequence (Bansal & Gefen, 2010; Malhotra, Kim, & Agarwal, 2004).

The privacy risks for cloud consumers may vary significantly with the privacy policies and terms of service offered by the cloud provider (Katzan, 2010; Rittinghouse & Ransome, 2017). The amount of privacy a cloud consumer has in a public cloud can therefore be "determined by the cloud service provider's agreement" (Pirrone & Trainor, 2013, p. 62). Nevertheless, from the point of view of the cloud consumer, there might be a constant concern about the capability of the cloud provider to ensure that "privacy is not compromised and data is not lost or misappropriated" (J. Kerr & Teng, 2012, p. 2). The main challenge for cloud providers could therefore be summarised as developing cloud services in such a way that privacy risks are reduced and legal compliance is ensured (Jaeger, Lin, & Grimes, 2008; Pearson, 2009; Rittinghouse & Ransome, 2017).

However, as shown in Figure 9, the privacy and data protection standards differ significantly between the USA and Germany. Forrester (2017) created this map based on the data of the U.S. Department of Commerce and country specific legislation, where the USA only has "minimal restrictions" and Germany is one of the "restricted" countries in terms of privacy and data protection standards. In all countries marked with a yellow exclamation mark, government surveillance may impact privacy.

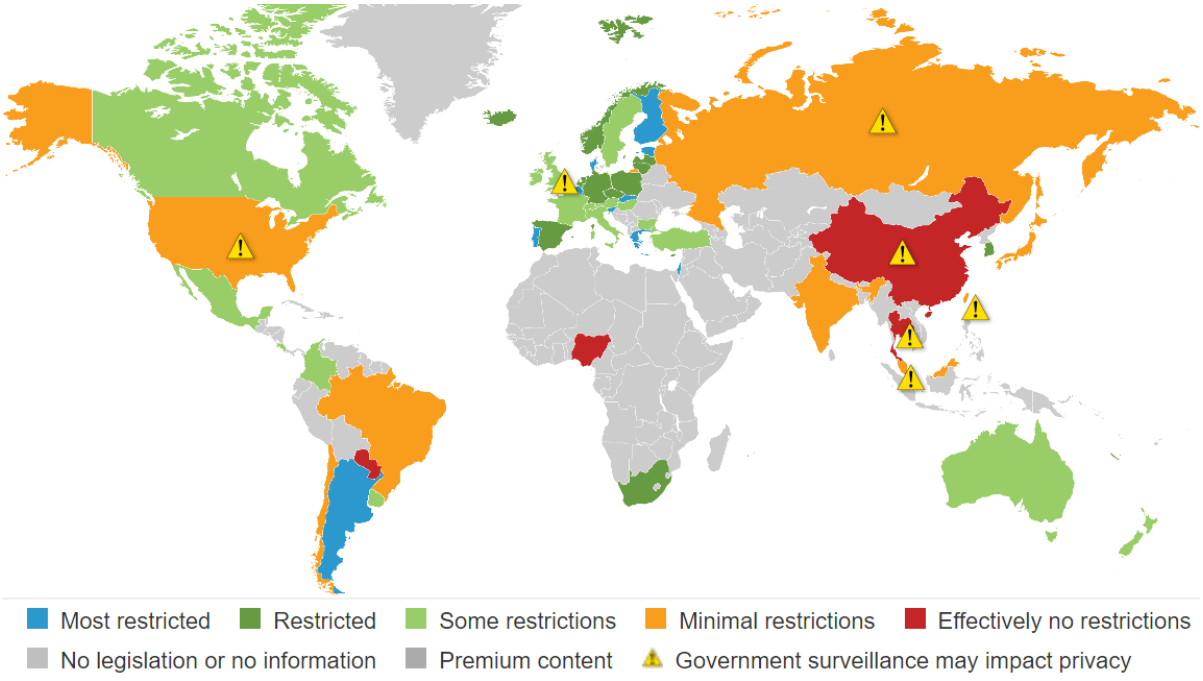


Figure 9: Privacy and data protection by country. Adapted from Forrester (2017).

This map by Forrester (2017) shows the levels of privacy and data protection standards before the implementation of the EU's General Data Protection Regulation (GDPR) on the 25th of May 2018. However, this should not have any impact on the difference of privacy and data protection standards between the U.S. and Germany. Additionally, all interviews for the current research were conducted prior to the renewed EU data protection standards. At the time of the interviews, the data protection rules of the EU member states were not harmonised, and the national implementations of the EU data protection directive differed between the countries. All EU member states had enacted their own data protection legislation based on the EU data protection directive. In Germany, the Bundesdatenschutzgesetz (BDSG), the German federal data protection act, in conjunction with the data protection acts of the German federal states, served to "implement directive 95/46/EC of the European Parliament" and to "protect the individual against his/her right to privacy being impaired through the handling of his/her personal data" (Germany, 2003, p. 1). The following Section 2.1.6.3 will provide additional information on GDPR.

Onwubiko (2010, p. 276) argued that privacy was already difficult to satisfy with traditional IT systems and that it was especially challenging with public clouds, where data can "traverse through geographical borders that impact both legal and regulatory requirements of the information being transported or stored". Public cloud computing

faces similar privacy issues as other IT service delivery models, but it can also "magnify existing issues" such as trans-border data flow restrictions and data processing in certain geographic locations (Pearson, 2012, p. 21). Additionally, if the data of an organisation is transferred to another legal jurisdiction, the company might need to verify if this "transfer violates the privacy laws of its home jurisdiction" (Rennie, 2010, p. 12).

Privacy in the cloud is hence protected in the best viable way if no personal data is transferred to, processed by or stored in the cloud platform (Martucci et al., 2012). Since this might not be possible for many companies, organisations might have to verify that their cloud provider meets all compulsory legal requirements. But even if no personal data will be saved in a public cloud, other data such as intellectual property and trade secrets may require confidentiality and protection on a similar or even higher level (Pearson, 2012; Wang et al., 2017). The threat of intellectual property theft and economic espionage are discussed in more detail in the findings and discussion chapters.

2.1.6.3 Regulations, policies and legal issues

The third critical aspect for public cloud computing adoption are regulations, policies and legal issues. The studies presented in Section 2.1.6 showed that unclear legal and regulatory requirements was one of the top obstacles for public cloud computing adoption and Marston et al. (2011) argued that further research needed to be conducted in international regulations and policies affecting public cloud computing.

Data that is stored in a public cloud may have more than one physical and legal location at the same time (Ruparelia, 2016; Subashini & Kavitha, 2011), can be managed by different entities (Katzan, 2010; Rittinghouse & Ransome, 2017), and is often difficult to locate where the data is physically stored (Pearson, 2012; Ruparelia, 2016). Additionally, cloud providers may themselves lease cloud computing services such as storage and computing capacity from other providers and re-sell a combined services package made of own and external resources (Pearson, 2012; T-Systems, 2017). Therefore, in an extreme case, the data can be stored on a server infrastructure of a third party outside the jurisdiction of both the cloud consumer and the cloud provider (Ruparelia, 2016). In the case of the current research, data of a German

company can be stored in a data centre in the EU (e.g. Ireland) and the data centres are owned by a U.S. company.

Furthermore, a cloud consumer may also violate local laws when data is transferred to and from the public cloud (Pearson, 2012). Due to the nature of the Internet, data transfer routes may change because of congestion or a malfunction of a network component, which makes it difficult to determine the borders that are crossed by the data. However, according to Pirrone and Trainor (2013, p. 59) laws that protect these communications “have not been updated in decades”. The fact that data transferred to and from cloud data centres needs to cross multiple networks was probably exploited by intelligence agencies that wiretapped several global internet hubs. The disclosure of these activities will be discussed in the following sections.

Nikoloff (2013) argued that the stricter the data protection regulations in one country are, the more stringent are the requirements for cross-border data transfers and the more unsure companies are about how to meet these requirements. This might be one of the reasons why some companies tend to take no chances and keep their data in their own data centre (Techconsult, 2013d). This relationship between legal uncertainties and the preference for private cloud services will also be covered in the findings and discussion chapters.

Several different regulations, policies and legal frameworks may apply to public cloud computing contracts between U.S. cloud providers and German companies (Borges, 2014; European Parliament, 2012). These include the EU data protection directive (European Commission, 1995; European Parliament, 1995; Reding, 2011), the Federal Data Projection Act of Germany (2003), the EU model clauses and additional sector/industry specific requirements. A review of these policies is not in the scope of this research. Additionally, many relevant policies are subject to constant change and the most current policies and versions should be reviewed by cloud consumers and cloud providers on a regular basis. One example is the U.S.-EU Safe Harbour framework (BfDI, 2010, 2011; ITA, 2000, 2014) which was replaced by the U.S.-EU Privacy Shield (European Commission, 2016). Another example is the EU’s General Data Protection Regulation (GDPR), which replaced the current EU data protection directive (European Parliament, 2016) on the 25th of May 2018.

The GDPR (EU 2016/679) is a new regulation in EU law on data protection and privacy for all individuals within the EU and the EEA that also addresses the export of personal data outside these areas. The primary goal of the GDPR was to strengthen citizens' and residents' online privacy rights and boost Europe's digital economy (European Commission, 2012a). Since the GDPR is a regulation and not a directive, it has direct legal effect throughout the EU and does not require transposition into national legislation (Blackmer, 2016). With the UK scheduled to leave the EU in 2019, the UK granted royal assent to the Data Protection Act 2018 on 23 May 2018, which allows for continuation of the GDPR after the exit (Pinsent Masons, 2018). IT companies including U.S. cloud providers adopted their services, procedures and contracts to meet the requirements of the GDPR (Amazon, 2018; Microsoft, 2018). According to a survey from Dimensional Research (2017), 83% of the respondents from large companies in the U.S. and Europe stated that their spending on GDPR compliance would be "six figures". Therefore, U.S. cloud providers had to make significant investments to be compliant with the data protection laws of their EU customers. Nevertheless, just hours after the official implementation of the GDPR, privacy activists sued Facebook and Google for allegedly violating the GDPR (Hern, 2018a). It remains to be seen if the GDPR will have a positive impact on the privacy concerns of cloud consumers regarding storing their data in public cloud services and might be a topic for future research.

The following sections will focus on the U.S. law enforcement initiatives which caused substantial concerns for potential German cloud consumer companies.

2.2 Global surveillance disclosures

Having discussed the relevant concepts, benefits and implications of cloud computing, the following two sections will give an overview of the events related to the global surveillance programmes of the U.S. government and its impact on cloud computing services. As argued in the following sections, the global surveillance disclosures caused great uncertainty among German citizens and companies as well as avoidance of U.S. online services. This will also become apparent in the analysis of the key informant interviews of the current research. Therefore, it is central for the current study to discuss the relevant background information on the global surveillance programmes.

Section 2.2.1 will focus on the U.S. government initiatives that were publicly known and discussed before the publications on the NSA global surveillance programmes. Section 2.2.2 will provide background information regarding the NSA global surveillance programmes revealed by Edward Snowden.

2.2.1 Pre-Snowden (2001-2013)

After the 9/11 terrorist attacks, to protect the U.S. against international terrorism (Bush, 2001), the powers of the U.S. law enforcement agencies have been significantly expanded (R. Anderson, 2008; Jaeger, Bertot, & McClure, 2003; E. C. Liu, 2011; K. C. Wong, 2006). A central element of this initiative was the USA PATRIOT Act of 2001, which, among other changes, granted federal officials greater authority to trace and intercept communications for law enforcement and foreign intelligence gathering purposes (Doyle, 2002). The acronym in USA PATRIOT Act stands for ‘‘Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism” and the objective of the act was to “deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes” (U.S., 2001, p. 272).

The USA PATRIOT Act of 2001 was enacted on the 26th of October 2001 and extended by the PATRIOT Sunsets Extension Act of 2011 (E. C. Liu, 2011). The USA PATRIOT Act conferred extensive powers on the U.S. law enforcement agencies inside the United States (Gershman, 2013), but also beyond its borders (R. Anderson, 2008; EFF, 2015; EPIC, 2015). However, the act itself only granted few new powers and could rather be seen as a framework which amends other laws (Van Hoboken et al., 2012). The most important supplementary acts relevant to this study are the Foreign Intelligence Surveillance Act of 1978 (FISA) (U.S., 1978) and the Electronic Communications Privacy Act of 1986 (ECPA) (U.S., 1986), which have been amended by the Protect America Act of 2007 (PAA) (U.S., 2007) and the FISA Amendments Act of 2008 (FAA) (U.S., 2008).

The FISA provided a framework by which government agencies, in the interest of national security, could be authorised to conduct electronic surveillance, perform physical searches, trap and trace devices, and access specific business records (E. C. Liu, 2011). The ECPA included three additional titles known as the Wiretap Act, the Stored Communications Act (SCA), and the Pen-Register Act, and addressed wire,

oral, and electronic communications that are being in transit or stored on a computer. Additionally, the PAA removed the requirement for the U.S. government to “obtain court orders to effectively collect foreign intelligence about foreign targets located in foreign locations” (Bush, 2007, p. 1).

One of the most controversial topics around the USA PATRIOT Act was related to the use of National Security Letters (NSLs) by the U.S. Federal Bureau of Investigation (FBI) (Böken, 2011; Eggen, 2007; E. C. Liu, 2011; Nieland, 2006; Pilkington, 2013). A NSL seeks information from financial institutions and communication providers in national security investigations (Doyle, 2014). Unlike FISA orders, NSLs could be issued directly by federal agency officials (E. C. Liu, 2011) and the recipients of a NSL were not allowed to disclose to anybody, including their lawyers, that they have received such request (Nieland, 2006). Section 505 of the USA PATRIOT Act further expanded the authorities that are allowed to issue NSLs to any special agent in charge at a FBI field office and, in some circumstances, also to federal agencies outside the FBI (E. C. Liu, 2011).

The USA PATRIOT Act amendments also changed the requirements for NSLs. Previously NSLs required a link to a foreign power or its agent, but after the reform it was sufficient when the requested information was relevant to an investigation against international terrorism or intelligence activities (Nieland, 2006). Following the adoption of the USA PATRIOT Act, the number of NSLs issued by the FBI had increased intensely (Nieland, 2006) from hundreds between 1978 and 2001 (*Doe v. Ashcroft*, 2004) to more than 30 000 NSLs per year between 2002 and 2005 (DOJ, 2007; Gellman, 2005).

The USA PATRIOT Improvement and Reauthorization Act of 2005 changed some of the NSL characteristics. Recipients of a NSL were now allowed to consult a lawyer and the FBI needed to justify each case that required secrecy (Nieland, 2006). However, U.S. courts have since been discussing if the use of secret NSL violates constitutional provisions on the separation of powers (*Doe v. Ganzales*, 2007; EFF, 2014; Misztal, 2013).

Another controversial aspect of the USA PATRIOT Act was related to Section 215 of the act, which broadened the access of federal officials to materials in investigations (E. C. Liu, 2011). Before the USA PATRIOT Act of 2001, only records from common

carriers, public accommodation facilities, storage facilities and vehicle rental facilities could be obtained (E. C. Liu, 2011). The USA PATRIOT Act of 2001 (U.S., 2001, p. 287) extended the scope to “any tangible things (including books, records, papers, documents and other items)”.

The PATRIOT Sunsets Extension Act of 2011 (U.S., 2011) extended the USA PATRIOT Improvement and Reauthorization Act of 2005 (U.S., 2005) and the Intelligence Reform and Terrorism Prevention Act of 2004 (U.S., 2004). The USA PATRIOT Act expired on the 1st of June 2015 and was replaced by the USA Freedom Act of 2015 (U.S., 2015), which was signed into law by President Obama on the 2nd of June 2015.

The USA Freedom Act promised to end the bulk collection of data, to prevent government overreach by prohibiting large-scale data collection and to allow challenges of national security letter gag orders. Critics, however, found that most of the changes relating to non-U.S. citizens were only cosmetic (Severson, 2015). Organisations like the Electronic Frontier Foundation (EFF) have described the USA Freedom Act as a step in the right directions that still had “serious faults that should be addressed” (Reitman, 2015, p. 1) and criticised that the act was not being applied in the right way (D. Greene, 2016). Likewise, the Centre for Constitutional Rights (CCR) stated that “the USA Freedom Act actually has produced only very marginal gains for privacy” (Kadidal, 2015, p. 3).

Table 9 provides an overview of some of the most important laws and bills around the USA PATRIOT Act. The table shows that the USA PATRIOT Act was changed and reauthorized several times and lasted for about 14 years.

Table 9: Timeline of laws and bills regarding the U.S. government surveillance activities

Date	Author(s)	Event
26 Oct 2001	U.S. (2001)	The USA PATRIOT Act of 2001 was enacted.
17 Dec 2004	U.S. (2004)	President George W. Bush signed the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), making it law.
3 Jan 2006	U.S. (2005)	The USA PATRIOT Act was reauthorized by the USA PATRIOT Improvement and Reauthorization Act of 2005.
5 Aug 2007	U.S. (2007)	The Protect America Act of 2007 (PAA) was signed into law by President George W. Bush.
9 Jul 2008	U.S. (2008)	President George W. Bush signed the FISA Amendments Act of 2008 (also called the Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008) into law.

26 May 2011	U.S. (2011)	The PATRIOT Sunsets Extension Act of 2011 extended the USA PATRIOT Improvement and Reauthorization Act of 2005 and the Intelligence Reform and Terrorism Prevention Act of 2004.
30 Dec 2012	U.S. (2012)	President Barack Obama signed H.R. 5949, the Foreign Intelligence Surveillance Act (FISA) Amendments Act Reauthorization Act of 2012 into law.
2 Jun 2016	U.S. (2015)	The USA PATRIOT Act expired on the 1st of June 2015 and was replaced by the USA Freedom Act which was signed into law by President Barack Obama on the 2nd of June 2015.

Since its implementation, the USA PATRIOT Act has been subject to continuous criticism from government officials, scholars and press representatives. In the U.S., the critics were typically related to the act being unconstitutional and to spying on U.S. citizens (R. Anderson, 2008). For example, U.S. phone carriers such as Verizon gave the U.S. government access to millions of U.S. customer records after the 2001 terrorist attacks. (Kushida, Murray, & Zysman, 2012).

In Europe, however, the USA PATRIOT Act became known for its potential access to European data stored in U.S. cloud computing environments (Batchelor, 2012; Rennie, 2010; R. Smith, 2009; Walden, 2012; Whittaker, 2012). The USA PATRIOT Act provided U.S. government entities with the option to force U.S. cloud providers to hand over data of their European customers (Bryant, 2013a; Dix et al., 2013; Kushida, Murray, & Zysman, 2011). U.S. cloud providers were requested to pass the requested data even if it was stored in a data centre outside the U.S. borders, for example in Dublin, Ireland (Böken, 2011; Manta, 2011; Stuart & Bromage, 2010). Furthermore, the U.S. cloud providers were not allowed to disclose to anybody, including their customers, that they have received such request (Andrikopoulos et al., 2013; Whittaker, 2011d).

Companies were told that if they wanted to avoid the reach of the USA PATRIOT Act they needed to make sure that neither the company itself nor their cloud computing service provider had any operations in the U.S. (Billings, 2012; Ouedraogo, Biennier, & Ghodous, 2013; Overby, 2012). The USA PATRIOT Act was therefore seen as a hurdle to international companies to adopt cloud computing services and caused insecurity and indignation among companies in Europe (Géczy et al., 2011; Kesan, Hayes, & Bashir, 2013; Lanois, 2010; Obeidat & Turgay, 2013).

However, the USA PATRIOT Act did not only raise concerns among businesses but also among academics (Gorham-Oscilowski & Jaeger, 2008). According to Whittaker

(2011a, p. 1), more than 300 universities in Europe had outsourced their student and staff email services to U.S. cloud providers and European universities were “risking their students' security by outsourcing to the cloud”. In November 2012, legal experts from the University of Amsterdam's Institute for Information Law published a research paper on the possibilities for the U.S. government to obtain access to information in the cloud from Dutch institutions on the basis of U.S. law, Dutch law and international co-operation (Van Hoboken et al., 2012). The authors concluded that the U.S. government could gain access to data from Dutch universities through a complex and dynamic system of national security and intelligence powers and their recommendation was that universities should take this risk into account in their cost-benefit analysis. The potential violation of privacy as a basic human right by the USA PATRIOT Act (Bowers, 2006) also raised “serious ethical concerns” among academics (Harris, Lang, Yates, & Kruck, 2011, p. 185).

As it will be outlined in the following section, the USA PATRIOT Act was only one of the most prominent instruments of the multiple means that U.S. government agencies could have used to gain access to data in foreign countries.

2.2.2 Post-Snowden (2013-present)

Since June 2013, international media organisations worldwide such as The Guardian and The Washington Post have revealed numerous operational details about the global surveillance programmes of the U.S. National Security Agency (NSA) and its international partners which have caused worldwide concerns over the methods and extent of global surveillance (Reding, 2013b; UN, 2013). The majority of those disclosures originate from thousands of intelligence files which have been copied and spread by the ex-NSA contractor Edward Snowden (Gellman, Blake, & Miller, 2013; Pincus, 2013).

The first documents that have been published revealed that the U.S. government required the telecommunications provider Verizon to hand over phone records of millions of Verizon customers under Section 215 of the USA PATRIOT Act (Greenwald, 2013b). One day later, Gellman and Poitras (2013) published NSA-internal PowerPoint slides which showed how the agency and international partners collected emails, chats, photos and other data from international sources under Section 702 of the FISA Amendment Act.

In the following months, many more publications followed that disclosed the extent of the collection of information by the NSA. Since not all publications could be discussed in detail in the background chapter of this research, Table 10 provides an overview of some of the major publications on the global surveillance disclosures. The table illustrates that most of the articles were published in 2013 and 2014 and only a few articles based on the Snowden documents were published at a later point in time.

Table 10: Timeline of global surveillance disclosures

Date	Author(s)	Title
6 Jun 2013	Greenwald (2013b)	NSA collecting phone records of millions of Verizon customers daily
7 Jun 2013	Gellman and Poitras (2013)	U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program
21 Jun 2013	MacAskill, Borger, Hopkins, Davies, and Ball (2013)	GCHQ taps fibre-optic cables for secret access to world's communications
7 Jul 2013	Timberg and Nakashima (2013)	Agreements with private companies protect U.S. access to cables' data for surveillance
12 Jul 2013	Greenwald (2013a)	Microsoft handed the NSA access to encrypted messages
31 Jul 2013	Greenwald (2013c)	XKeyscore: NSA tool collects 'nearly everything a user does on the internet'
2 Aug 2013	Ball, Harding, and Garside (2013)	BT and Vodafone among telecoms companies passing details to GCHQ
29 Aug 2013	Gellman and Miller (2013)	U.S. spy network's successes, failures and objectives detailed in 'black budget' summary
5 Sep 2013	Perlroth, Larson, and Shane (2013)	N.S.A. Able to Foil Basic Safeguards of Privacy on Web
14 Oct 2013	Gellman and Soltani (2013a)	NSA collects millions of e-mail address books globally
23 Oct 2013	Appelbaum, Stark, and Rosenbach (2013)	Did US Tap Chancellor Merkel's Mobile Phone?
25 Oct 2013	Ball (2013)	NSA monitored calls of 35 world leaders after US official handed over contacts
27 Oct 2013	Appelbaum, Blome, et al. (2013)	Embassy Espionage: The NSA's Secret Spy Hub in Berlin
30 Oct 2013	Gellman and Soltani (2013b)	NSA infiltrates links to Yahoo, Google data centres worldwide, Snowden documents say
4 Dec 2013	Gellman and Soltani (2013c)	NSA tracking cell phone locations worldwide, Snowden documents show
10 Dec 2013	Soltani, Peterson, and Gellman (2013)	NSA uses Google cookies to pinpoint targets for hacking
20 Dec 2013	Menn (2013)	Exclusive: Secret contract tied NSA and security industry pioneer
29 Dec 2013	Appelbaum, Poitras, et al. (2013)	Inside TAO: Documents Reveal Top NSA Hacking Unit
16 Jan 2014	Ball (2014)	NSA collects millions of text messages daily in 'untargeted' global sweep

27 Jan 2014	Glanz, Larson, and Lehren (2014)	Spy Agencies Tap Data Streaming from Phone Apps
30 Jan 2014	Vidal and Goldenberg (2014)	Snowden revelations of NSA spying on Copenhagen climate talks spark anger
4 Feb 2014	Oltermann (2014)	NSA tapped German ex-chancellor Gerhard Schröder's phone – report
12 Mar 2014	R. Gallagher and Greenwald (2014)	How the NSA Plans to Infect 'Millions' of Computers with Malware
18 Mar 2014	Gellman and Soltani (2014)	NSA surveillance program reaches ‘into the past’ to retrieve, replay phone calls
29 Mar 2014	Poitras, Rosenbach, and Stark (2014)	GCHQ and NSA Targeted Private German Companies and Merkel
14 May 2014	S. Gallagher (2014)	Photos of an NSA “upgrade” factory show Cisco router getting implant
6 Jun 2014	Garside (2014)	Vodafone reveals existence of secret wires that allow state surveillance
19 Jun 2014	Geist, Gjerding, Moltke, and Poitras (2014)	NSA ‘third party’ partners tap the Internet backbone in global surveillance program
4 Jul 2014	BBC (2014a)	Germany arrests man suspected of spying for US
25 Aug 2014	R. Gallagher (2014)	The Surveillance Engine - How the NSA Built Its Own Secret Google
19 Feb 2015	Scahill and Begley (2015)	The Great SIM Heist – How Spies Stole the Keys to the Encryption Castle
16 Aug 2016	Solon (2016)	Hacking group auctions 'cyber weapons' stolen from NSA
7 Dec 2016	Follorou (2016)	American and British spy agencies targeted in-flight mobile phone use

According to Gellman and Poitras (2013), the internet services of U.S. technology companies such as AOL, Apple, Facebook, Google, Microsoft and Yahoo were a major target of the NSA surveillance programme. Early publications suggested that these internet companies had in some way collaborated with the NSA (Gellman, Soltani, & Peterson, 2013; Greenwald, 2013a; Menn, 2013; Pirrone & Trainor, 2013) and that the agency had direct access to their servers. The reports also suggested that the NSA (Timberg & Nakashima, 2013) and its international partners (MacAskill et al., 2013) collaborated with the world’s leading telecoms firms (Ball, Harding, et al., 2013) to gain access to undersea fibre-optic cables (Appelbaum, Poitras, et al., 2013) in order to collect, store and analyse the global telephone and internet traffic (Gellman & Soltani, 2014; Greenwald, 2013c; Soltani & DeLong, 2013).

However, later reports claimed that the NSA collected the vast majority of the data without the knowledge and consent of the IT companies and telecommunications provider (Levy, 2014). For example, the NSA and international partners were accused to have bypassed data encryption technologies (Perlroth et al., 2013) and intercepted

internet communications between data centres (Gellman & Poitras, 2013; Gellman & Soltani, 2013b) to gather thousands of emails per day (Gellman & Soltani, 2013a) and other information (Ball, Borger, & Greenwald, 2013).

Edward Snowden handed all documents and data to selected journalists in the U.S., UK and Germany. The original files were not made publicly available. Hence it is difficult for scholars to verify the accuracy of the findings published by the press. Nevertheless, as shown in the following sections, the result of the extensive press coverage of the Snowden revelations was a broad public awareness of the NSA global surveillance activities.

2.3 A matter of trust

The following sections will summarize the reactions of government officials, German companies, U.S. cloud providers and German cloud providers to the global surveillance disclosures.

2.3.1 Government reactions

The global surveillance disclosures had a direct negative impact on the trust in the U.S. government and U.S. intelligence work (Mascolo & Scott, 2013; Schneier, 2013; Smale, 2013; Stiglitz, 2013) and even caused social movements against mass surveillance such as Stop Watching Us (2013), The Day We Fight Back (2014) and Restore the Fourth (2016).

The indignation surrounding the global surveillance disclosures also had an influence on the political agenda of the EU regarding cloud computing adoption. Already before the revelations by Edward Snowden, the dominance of the U.S. in the cloud computing industry has led to various actions on the level of the EU government and on national levels. In 2012, the European Commission published a paper titled “Unleashing the Potential of Cloud Computing in Europe” to promote cloud computing in the EU by introducing common standards, fair contract terms, and a European Cloud Partnership (ECP) (European Commission, 2012d). In this paper the EC was “quite frank about their intentions” (Castro, 2013, p. 2) of “building a new industry, and better competing against the United States in particular” (European Commission, 2012e, p. 2) to “become a world cloud computing powerhouse” (European Commission, 2012d, p. 16). According to a study performed by European Commission (2012c) on behalf of

the European Commission, the intended policy actions would have a significant impact on cloud computing adoption in Europe. The estimates published in the study indicated that by 2020, cloud computing revenues could rise to approximately 80 billion Euros following a full implementation of the strategy, compared to only 35 billion Euros of cloud revenues in a scenario without EU government interventions (European Commission, 2012e). In terms of job creation potentials, European Commission (2012c) expected 3.8 million new jobs to be generated in the EU in a policy-driven scenario, against 1.3 million new jobs without interventions.

In a follow-up study published in June 2015, the authors acknowledged that the assumptions of the first study “were shown to be too optimistic” (European Commission, 2015b, p. 72). They cited a number of reasons why more recent estimates were lower, including the early stage of the “cloud diffusion curve”, the economic crisis across Europe, and the overall more pessimistic perspectives of development and growth in Europe (European Commission, 2015b, p. 72). Additionally, the 2012 report was commissioned to estimate the impact of government policies on the cloud computing market, whereas the follow-up study only focused on a baseline, optimistic and pessimistic calculation. The authors also stated that some of the policies proposed in the first report have already been adopted by member states. Although not specifically addressed in the report, it could be argued that the first report was politically motivated to promote policy changes in the EU to catch up with the U.S. information technology economy.

However, after the first revelations of the NSA global surveillance activities, the political leaders of the EU openly addressed the loss in trust of the EU in the U.S. government and the consequential repercussions for cloud computing adoption in Europe (European Parliament, 2013). In July 2013, the EU's home affairs commissioner, Cecilia Malmström, wrote to senior U.S. officials that "mutual trust and confidence have been seriously eroded” and that she expected the U.S. to “do all that it can to restore them” (Croft, 2013). In the same week, the European Commissioner for Digital Agenda, Neelie Kroes, directly addressed the consequences of the lack of trust for U.S. cloud services:

> *“If European cloud customers cannot trust the United States government or their assurances, then maybe they won't trust US cloud providers either. That*

> *is my guess. And if I am right then there are multi-billion euro consequences for American companies." (European Commission, 2013f, p. 2)*

She stated that privacy was "not only a fundamental right" but could "also be a competitive advantage" and European cloud providers "should take advantage of interest to provide services with better privacy protection". Kroes added that "cloud has a lot of potential", but that "potential doesn't count for much in an atmosphere of distrust" (European Commission, 2013f, p. 2).

End of October 2013, all 28 EU leaders signed a statement that addressed the NSA surveillance activities in which they stated that "a partnership must be based on respect and trust" and that "a lack of trust could prejudice the necessary cooperation in the field of intelligence gathering" (European Council, 2013, p. 19). A few months later, in February 2014, the European Parliament published a report on the NSA surveillance programme and noted that

> *"trust in US cloud computing and cloud providers has been negatively affected by the above-mentioned practices; emphasises, therefore, the development of European clouds and IT solutions as an essential element for growth and employment and for trust in cloud computing services and providers, as well as for ensuring a high level of personal data protection" (European Parliament, 2014a, p. 30).*

Furthermore, the European Parliament (2014a, p. 30) called "on all public bodies in the Union not to use cloud services where non-EU laws might apply.

In the following months after the NSA global surveillance disclosures, the EU has been evaluating possible consequences for the transatlantic relationship with the U.S. (Dix et al., 2013; European Commission, 2013d, 2013e; European Parliament, 2014b; Reding, 2013c). This also included the negotiations on the Transatlantic Trade and Investment Partnership (TTIP) between the U.S. and the EU (Deutsche Welle, 2016; Hilary, 2015; O'Brien). Moreover, the EU decided to unify and strengthen data protection for EU citizens (Reding, 2013a). As stated above, on the 27th of April 2016, the European Parliament (2016) approved the new General Data Protection

Regulation (GDPR). It enters into application on the 25th of May 2018 and will replace the data protection directive (Cate, 1994; European Commission, 1995). To comply with GDPR, U.S. cloud providers will presumably need to make significant changes to their service terms and operations (Coles, 2014; Donnelley, 2015; Lauchlan, 2016; Voigt & von dem Bussche, 2017).

Another example is the U.S.-EU "Safe Harbour" arrangement (European Commission, 2012b), which was created to bridge the gaps in privacy law between the U.S. and the EU and provide a way for U.S. companies to reach an acceptable level of personal data protection as required by the EU Data Protection Directive (European Commission, 2000, 2009). However, the U.S.-EU Safe Harbour framework has been subject to substantial criticism from EU and German government bodies since its introduction (Connolly, 2008; Marnau & Schlehahn, 2011; Pechardscheck & Schiefer, 2012). In two reports commissioned by the European Parliament, the European Commission (2002, p. 10) concluded that a substantial number of U.S. organisations that have signed up for the Safe Harbour programme were "not observing the expected degree of transparency" or had published a policy which was not compliant with the Safe Harbour principles (European Commission, 2004). In November 2013, after the NSA surveillance disclosures, the European Commission (2013b) published "a real to-do list" (Reding, 2014, p. 2) with thirteen specific recommendations to the U.S. authorities which were expected to be implemented by summer 2014. However, in October 2015, following constant criticism expressed by the general public (Chaffin, 2013; Dhont, Asinari, & Poullet, 2004; Millard, 2013), the Court of Justice of the European Union declared the Commission's 2000 decision on EU-U.S. Safe Harbour invalid (European Commission, 2015a). A few months later, in February 2016, the European Commission and the United States agreed on the EU-U.S. Privacy Shield as a new framework for transatlantic data transfers (European Commission, 2016). In October 2017, the European Commission (2017) published its first annual report on the functioning of the EU-U.S. Privacy Shield and concluded that it ensured an adequate level of protection for the personal data transferred from the EU to participating companies in the U.S. but also suggested a number of recommendations to further improve the application of the agreement.

Table 11 highlights some of the reactions by European Union, German and U.S. government officials. In comparison with the dates of the press releases listed in the previous section, corresponding government policies such as the EU-U.S. Privacy Shield or the General Data Protection Regulation (GDPR) took several years to be approved and will take additional years to be implemented.

Table 11: Timeline of government reactions

Date	Author(s)	Event
15 Jan 2012	European Commission (2012a)	The European Commission proposed a comprehensive reform of the EU's data protection rules to strengthen online privacy rights and boost Europe's digital economy.
19 Jan 2012	Kenneth (2012)	U.S. officials dismissed cloud privacy issues in relation to the USA PATRIOT Act.
6 Sep 2012	Sayer (2012)	The French government announced to invest in two local cloud computing providers.
27 Dec 2012	European Commission (2012d)	The European Commission published a paper on the potential of cloud computing and called upon the EU member states to embrace the potential of the technology.
4 Jul 2013	European Commission (2013f)	The European Commissioner for Digital Agenda encouraged European cloud providers to take advantage of interest to provide services with better privacy protection.
5 Jul 2013	Croft (2013)	The EU threatened to suspend agreements granting the U.S. access to European financial and travel data.
23 Oct 2013	Deutsche Welle (2013c)	German chancellor Angela Merkel telephoned U.S. president Barack Obama to ask for an explanation about allegations that she was spied upon.
25 Oct 2013	European Council (2013)	All 28 EU leaders signed a statement that addressed the NSA surveillance activities.
27 Nov 2013	European Commission (2013c)	The European Commission appealed to the U.S. to restore trust in EU-U.S. data flows.
29 Jan 2014	Bundesregierung (2014)	German chancellor Angela Merkel warned the U.S. over consequences of surveillance activities in her first speech of her third term.
21 Feb 2014	European Parliament (2014a)	The European Parliament released a report of its inquiry into the NSA activities.
26 Jun 2014	Severin (2014)	The German government cancelled all contracts with Verizon because of the NSA surveillance activities.
6 Oct 2015	CJEU (2015)	The Court of Justice of the European Union declared the Commission’s 2000 decision on EU-U.S. Safe Harbour invalid.
6 Nov 2015	European Commission (2015a)	Following the judgement by the Court of Justice, the European Commission adopted a communication on the transfer of personal data from the EU to the U.S. under Directive 95/46/EC.
2 Feb 2016	European Commission (2016)	The European Commission and the United States agreed on the EU-U.S. Privacy Shield as a new framework for transatlantic data transfers.
27 Apr 2016	European Parliament (2016)	The European Parliament adopted the General Data Protection Regulation (GDPR).

The notion of trust was also a central theme in the reactions of German government officials. In July 2013, after the first revelations of the NSA surveillance activities, German chancellor Angela Merkel defended the practices of the U.S. government agencies and stated that preventing terrorist attacks was not possible "without the possibility of telecommunications monitoring" (Spiegel Online, 2013, p. 1). Likewise, German interior minister Hans-Peter Friedrich justified the NSA surveillance with the fight against terrorism and claimed that five terrorist attacks in Germany were prevented due to information from U.S. intelligence agencies (Deutsche Welle, 2013b).

However, in October 2013, after German chancellor Angela Merkel had been given information that the NSA was spying on her mobile phone communications, she called U.S. president Barack Obama to ask for an explanation (Appelbaum, Stark, et al., 2013). One day later, foreign minister Guido Westerwelle met the U.S. ambassador to Germany, John B. Emerson, to discuss the allegations. He stated that "spying on close friends and partners is totally unacceptable" and that "this undermines trust" and can harm the U.S.-Germany friendship" (Deutsche Welle, 2013a).

In January 2014, in her first speech of her third time in office, German chancellor Angela Merkel emphasised that trust has been profoundly shaken between the two transatlantic partners. She said that

> *"a programme in which the end justifies all means, in which everything that is technically possible is then acted out, violates trust and spreads mistrust" (Bundesregierung, 2014, p. 8).*

The NSA global surveillance scandal also had an impact on the opinion of German politicians about cloud computing services from U.S. providers (Neuerer, 2013). The German Minister of the Interior had suggested that "whoever fears their communication is being intercepted in any way should use services that don't go through American servers" (AP, 2013, p. 1). A few weeks later, the conference of German Federal and State Data Protection Commissioners decided that the authorities would "not issue any new permission for data transfer to non-EU countries (for example also for the use of certain cloud services)" (BfDI, 2013, p. 2). The Minister of Justice for the German state of Hessen even called for a boycott of U.S. technology

companies (Prodhan & Davenport, 2013). Furthermore, leading German politicians demanded a “Schengen Cloud” to create a trustworthy network between the countries in the Schengen Area in Europe (Volmer, 2013).

The U.S. government on the other hand did not seem to share the concerns of the European countries. In 2003, before the revelations of the NSA surveillance programmes, Professor O. Kerr (2003) from the George Washington University Law School claimed that the common perception of the USA PATRIOT Act was wrong. He argued that the USA PATRIOT Act only made minor changes to the U.S. electronic surveillance law and even “added several key privacy protections” (O. Kerr, 2003, p. 1). In his opinion, the USA PATRIOT Act was not perfect, but it was also not “the Big Brother law that many have feared” (O. Kerr, 2003, p. 2). In January 2012, two senior Obama administration officials called the USA PATRIOT Act controversy “overblown” and added that “any notion that the United States doesn't value privacy is mistaken" (Kenneth, 2012).

After the disclosures by Edward Snowden, the reactions of U.S. government officials were mixed. Congressman Jim Sensenbrenner (2013), who was one the authors of the USA PATRIOT Act, acknowledged that the act was misused by U.S. government surveillance agencies. Likewise, Senate Intelligence Committee Chairman Dianne Feinstein (2013) stated that she opposed the collection of phone records of U.S. allies and that she applied for a review of all U.S. intelligence surveillance programmes. In January 2014, U.S. President Barack Obama (2014) gave a public speech on the NSA mass surveillance activities. In his speech he promised to increase the restrictions on data collection of U.S. citizens but did not guarantee any protection of international data (The New York Times Editorial Board, 2014). U.S. technology companies including Facebook, Google and Yahoo criticized Obama’s speech for being too vague and for not going far enough to win back the trust of their users overseas (Guynn, 2014). A few days later, whilst the U.S.-Germany relations hit a new low (Lamarque, 2014), Obama gave an exclusive interview on German TV, addressing the concerns of German citizens regarding the U.S. surveillance programmes (A. Thomas, 2014). During the interview with the ZDF (2014, p. 1) he admitted that "a lot of suspicion had been built up in Germany” and that it would “take some time to win back trust".

In a survey conducted by Pew Research Center in November 2014-January 2015, only 43% of U.S. adults surveyed answered that it was unacceptable to monitor the leaders of other countries (G. Gao, 2015). Yet, 61% said it was unacceptable for the government to monitor the communications of U.S. citizens. However, 90% of German respondents answered that it was unacceptable to monitor foreign leaders and 78% said that it was unacceptable to monitor U.S. citizens.

As discussed above, the reactions of government officials were divergent. It could be argued that, while EU and German government officials highlighted the breach of trust and demanded consequences regarding the surveillance activities, the U.S. government representatives tried to downplay the incidents and attempted to justify the surveillance scope and methods. This conflicting view on the matter might be related to cultural differences between the countries, which will be discussed in the following chapters.

The following section will detail the reactions of German companies to the NSA global surveillance scandal regarding public cloud services adoption.

2.3.2 German company reactions

As detailed in Section 2.1.5, German companies are comparably reluctant with the adoption of public cloud computing services. One of the main reasons might be insufficient trust in cloud computing services, particularly from U.S. cloud providers. Already before the first reports about the powers of the USA PATRIOT Act appeared in the media, moving company data to the cloud was “a question of trust” (Everett, 2009, p. 6).

However, after the first U.S. cloud providers acknowledged the fact that U.S. cloud providers could be forced to disclose private and confidential data to the U.S. government (Whittaker, 2011c), the potential release of data to U.S. government entities through the USA PATRIOT Act (CSA, 2011; Martucci et al., 2012) emerged as one of the top concerns among IT directors of companies in the EU (Taylor, 2011). German companies were particularly concerned about the data privacy and data protection issues in conjunction with the USA PATRIOT Act (Experton, 2012; Pearson, 2012).

Following the reports on the potential access of the U.S. government to records in European data centres (Böken, 2011; Hackmann, 2012; Overby, 2012; Whittaker, 2011b), one of the main topics of the world's largest computer exposition CeBIT in Hannover in 2012 was trust (Der Tagesspiegel, 2012). In an interview during the exposition, the president of Germany's information and communication technology association BITKOM, Dieter Kempf, said that trust was an essential criterion for public cloud computing and that the USA PATRIOT Act was at the centre of the current data privacy discussions (Der Tagesspiegel, 2012). Other authors also highlighted the relevance of trust for German cloud consumers. In their reports on cloud computing trust, BearingPoint stated that sustainable cloud computing business relationships were founded on trust (Pechardscheck & Schiefer, 2012, p. 7) and that the main reason why many companies in Europe and Germany were failing to "tap into the huge opportunities offered by cloud computing" was a "lack of trust" (Nikoloff, 2013, p. 1).

In March 2013, Columbus (2013, p. 1) argued that cloud computing was "slowly winning the trust war" and that trust was "the greatest accelerator there is in cloud computing's growing adoption". However, in Summer 2013, a scholarly study with IT experts revealed that 89% of the respondents answered that the risk of the U.S. government to access company data through the USA PATRIOT Act has a "high to medium impact on successful cloud adoption" (Dutta et al., 2013, p. 44). In June 2013, just before the NSA PRISM disclosures by Edward Snowden, PricewaterhouseCoopers published a survey with 60 respondents from cloud provider companies that were active in the German market, predominantly decision makers from executive management (PwC, 2013a). The study revealed that, already before the news about the NSA practices spread in Germany, 75% of the cloud providers had been approached by cloud consumers regarding the USA PATRIOT Act. In the same study, more than half of the cloud providers also stated that the possibility of authorities accessing data was a "big" or "very big" problem for cloud consumers (PwC, 2013a).

The news around the NSA global surveillance activities have reinforced the concerns of European and German companies (Bryant, 2013d; Computerwoche, 2013; R. King, 2014; Meyer, 2013; Prodhan & Davenport, 2013; Shahani, 2014; Traynor, 2013). Several international surveys showed that non-U.S. companies, and particularly German companies, did not trust U.S. cloud services and preferred to keep their data

in their own data centres. In a survey conducted by the Cloud Security Alliance (CSA) in July 2013, 56% of the non-U.S. respondents stated that they would less likely use U.S.-based cloud providers because of the information leaked by Edward Snowden (CSA, 2013). Another 10% of the respondents even “cancelled a project to use US-based cloud providers” (CSA, 2013, p. 2). Moreover, a survey of 300 UK and Canadian companies revealed that the NSA scandal motivated 25% of those companies to move their data outside the U.S. (Peer1, 2014).

In a global survey with 23,376 Internet users from 24 countries (CIGI-Ipsos, 2014), German respondents had the least trust in Internet security (Greis, 2014). Of all 24 countries, Germany was the last in the list who believed that personal information on the Internet was secure (15%), the last who trusted international technology companies to play an important role in running the Internet (23%), and the last who would trust the United States to play an important role in running the Internet (13%). On the other hand, as illustrated in Figure 10, Germany was top on the list of the people who have heard about Edward Snowden (94%).

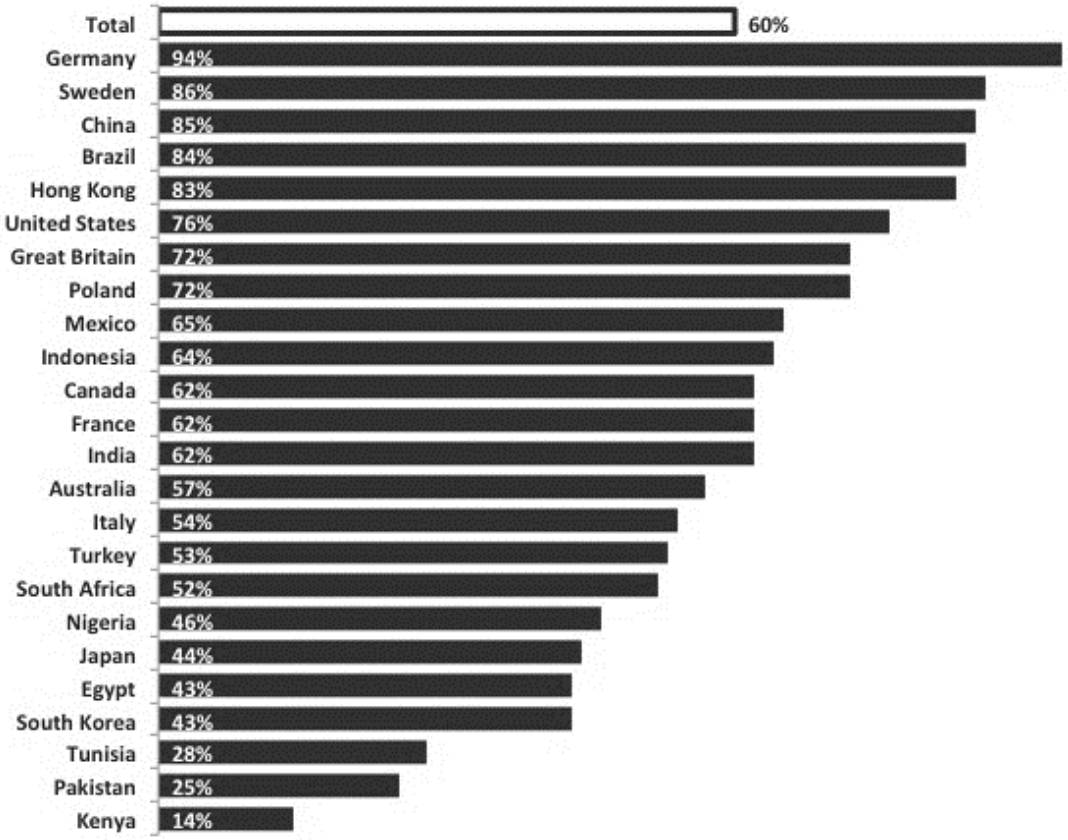


Figure 10: Respondents that heard about Edward Snowden. Adapted from CIGI-Ipsos (2014).

An international study with 1,000 IT decision makers conducted by NTT (2014) came to a similar result where about 100% of the respondents from Germany had at least some knowledge about the U.S. global surveillance programmes. In the same study, 87% of the respondents agreed that the Snowden revelations had changed their approach to cloud computing to some extent and about 19% of the German participants responded that the NSA surveillance programmes caused them to postpone or cancel their cloud computing projects (NTT, 2014).

According to the authors of the study from KPMG (2014, p. 37), German companies were “in general highly sensitive” in questions regarding data security. The authors concluded that the NSA espionage incidents have “increased this sensibility” and “reinforced existing reservations” about cloud computing (KPMG, 2014, p. 37). In response to the question how the cloud market will develop, 35% of the cloud providers surveyed in the study of PwC (2013a, p. 31) answered that “in Germany, for cultural reasons, customers will remain reluctant to embrace cloud computing for a long time”. The influence of the German and the U.S. culture on the adoption of U.S. cloud services by German companies will be further debated in the discussion chapter.

The global surveillance scandal also had a negative impact on the trust of SMEs in cloud services from U.S. providers (Steinhaus, 2013; Techconsult, 2013a). In a study with SMEs in Germany, more than half of the respondents stated that they only consider public cloud service providers which were registered and based in Germany (Techconsult, 2013c). The Snowden revelations were also named as a reason why German SMEs preferred a private cloud instead of a public cloud solution. Despite the higher costs of private cloud deployment models (see Section 2.1.3), 58% of the German SMEs favoured a private cloud setup (Techconsult, 2013d). This preference for private cloud setups will also be addressed in the findings and discussion chapters.

2.3.3 U.S. cloud provider reactions

Microsoft was one of the first public cloud provider that openly admitted that the data in their European data centres was subject to the USA PATRIOT Act (Kenneth, 2012). In 2011, Microsoft explained that because they had to comply with U.S. laws they could not guarantee that data stored in their EU-based data centres would not leave the European Economic Area (Whittaker, 2011c). This statement has reportedly caused a great stir among German companies (Böken, 2011). Two months later,

Google also admitted that the U.S. government had access to data stored outside the U.S. and that Google had received requests for European data from U.S. intelligence agencies (Stölzel, 2011). While the powers of the USA PATRIOT Act became a major topic among IT professionals in Europe and Germany (see Section 2.3.2), the impact on the cloud services business of U.S. providers was not quantifiable.

The NSA surveillance disclosures, however, had apparently a direct impact on the U.S. cloud industry (Messmer, 2013; Thibodeau, 2013) with significant monetary implications (Donohue, 2015; Gustin, 2013; Heuer, 2014). In August 2013, the Information Technology and Innovation Foundation (ITIF), a U.S. non-profit public policy think tank, published a report on the projected costs of the NSA PRISM scandal to the U.S. cloud computing industry. According to the ITIF, the U.S. cloud computing industry would lose between $22 billion and $35 billion U.S. dollars over the next three years after the revelations about the NSA surveillances programmes (Castro, 2013). A few days later, Forrester Research concluded that the estimate of the ITIF was too low. They estimated a net loss for cloud service providers of about $180 billion, a 25% decline in the overall IT services market (Staten, 2013). The New America's Open Technology Institute argued that, as a result of the NSA surveillance (Mascolo & Scott, 2013), the "trust in American businesses has taken a significant hit" (R. Greene, Kehl, Morgus, & Bankston, 2014, p. 7) and that the cloud computing industry was "particularly vulnerable and could lose billions of dollars in the next three to five years" (R. Greene et al., 2014, p. 2). An international cross-industry study conducted by El-Gazzar et al. (2016, p. 78) also found a "Snowden effect, an increased awareness about the threats that foreign governments may pose to data security", which may influence enterprise cloud adoption decisions.

U.S. cloud providers reportedly had to make significant investments in new data centres outside the U.S., in new encryption technologies and in other measures to address the concerns of their non-U.S. customers (Boulton, 2016; Scott, 2016). IBM (2014) invested more than one billion U.S. dollars in building new data centres in Europe, Asia and other regions outside the U.S. borders. Google invested in encrypting all network traffic between their data centres (Timberg, 2013) and Microsoft partnered with 21Vianet in China (Meisner, 2014) and T-Systems in Germany (Microsoft, 2015) to build highly secure cloud data centres that the U.S. government

“can’t touch” (Moody, 2015, p. 1). Castro (2013) argued that, in order to retain market share in a rapidly growing industry such as cloud computing, U.S. cloud providers not only have to keep existing customers, they also need to actively gain new customers. Consequently, if the U.S. cloud providers lose market share in the short term because of a lack of trust by their customers, this will have long term implications on their competitiveness in the cloud computing industry (Castro, 2013).

However, the global surveillance scandal might not only have had a negative impact on the sales figures of cloud service providers but also on other U.S. high technology enterprises. A variety of companies including Cisco, Citrix, HP, IBM, Intel and Qualcomm reported declining sales due to the NSA disclosures (S. Gallagher, 2013) or they reported that their products did not get approvals in foreign countries (Enderle, 2015).

The NSA surveillance disclosures caused the U.S. high technology and cloud provider industry to take a stand on the matter and to act to secure their business. Table 12 provides a timeline of the some of the most significant reactions by U.S. cloud providers. As discussed in the previous sections, most of the surveillance activities were disclosed in 2013 and 2014. However, as listed in Table 12, U.S. cloud providers are continually developing new measures to protect the data of their customers from government access and are challenging current legislations and legal practices.

Table 12: Timeline of U.S. cloud provider reactions

Date	Author(s)	Event
28 Jun 2011	Whittaker (2011c)	Microsoft admitted that the data in their European data centres was subject to the USA PATRIOT Act.
6 Aug 2011	Stölzel (2011)	Google admitted that the U.S. government has access to data stored outside the USA.
14 Jun 2013	McCullagh (2013)	Facebook and Microsoft disclosed the total number of legal orders they received.
17 Jun 2013	M. Mayer and Bell (2013)	Yahoo joined other U.S. technology companies in revealing U.S. surveillance requests.
18 Jul 2013	CDT (2013)	Major U.S. technology companies sent a letter to the U.S. congress and the president with a request to be allowed to publish detailed statistics about the types of national security requests.
05 Aug 2013	Castro (2013)	The Information Technology and Innovation Foundation (ITIF) published a report on the projected costs of the NSA PRISM scandal to the U.S. cloud computing industry.
14 Aug 2013	Staten (2013)	Forrester Research concluded that the estimate of the ITIF was too low.
09 Sep 2013	Google (2013b)	Google filed an amended petition in the U.S. Foreign Intelligence Surveillance Court and requested to be allowed to publish detailed statistics about national security requests.

11 Sep 2013	Rushe (2013)	Facebook criticised the U.S. government for their global surveillance practices.
14 Nov 2013	Google (2013a)	Google announced that government requests for user information have doubled over three years.
8 Dec 2013	Reform Government Surveillance (2013)	AOL, Apple, Facebook, Google, LinkedIn, Microsoft, Twitter and Yahoo created the ReformGovernmentSurveillance.com platform and sent an open letter to the president of the United States and the members of congress with a formal request to reform the U.S. government surveillance practices worldwide.
17 Jan 2014	IBM (2014)	IBM announced that they would invest more than one billion U.S. dollars in building new data centres in Europe, Asia and other regions outside the U.S.
3 Mar 2014	Curtis (2014)	Salesforce announced that they planned to open three new data centres in Europe.
18 May 2014	D. Thomas and Waters (2014)	Cisco wrote an open letter to President Barack Obama warning of a collapse of trust in U.S. technology.
30 Jun 2014	Hattem (2014)	The U.S. cloud provider ServInt announced that the number of their international customers went down by 50% due to the NSA surveillance revelations.
29 Jul 2014	R. Greene et al. (2014)	The New America Foundation publishes a report on the NSA's impact on the U.S. economy.
15 Aug 2014	Shih and Carsten (2014)	Apple announced that they would keep the personal data of Chinese users on encrypted servers in mainland China.
23 Oct 2014	Amazon (2014)	Amazon announced to open data centres in Germany.
19 May 2015	Reform Government Surveillance (2013)	The ReformGovernmentSurveillance.com group sent a second letter urging the members of the U.S. senate to pass the USA Freedom Act to prevent the bulk collection of internet metadata and to increase transparency about government demands for user information.
11 Nov 2015	Microsoft (2015)	Microsoft announced plans to offer cloud services from German data centres where Deutsche Telekom will control and oversee all access to customer data.
16 Feb 2016	Apple (2016)	Apple rejected to build a version of their mobile operating system that bypasses device security and creates a backdoor.
14 Apr 2016	J. Greene and Barrett (2016)	Microsoft sued the U.S. government over the frequent use of National Security Letters.
14 July 2016	Wingfield and Kang (2016)	Microsoft won an appeal over a U.S. search warrant that aimed to force Microsoft to turn over data stored in a data centre in Dublin.
24 Jan 2017	Stempel (2017)	The federal appeals court refused to reconsider its landmark decision forbidding the U.S. government from forcing Microsoft to turn over customer emails stored on servers outside the United States.

Several senior executives of those companies directly addressed the lack of trust of their customers in U.S. internet technologies. Microsoft's Chief Legal Officer Brad Smith stated that "people won't use technology they don't trust" and that the U.S. government needed to help restoring it (Meisner, 2013, p. 1). According to the CEO of Facebook, Mark Zuckerberg, the response of the U.S. government did not build "confidence in American internet companies" (Rushe, 2013, p. 1). The CEO of Yahoo, Marissa Mayer, said that the surveillance activities of the U.S. government had

“shaken the trust” of their users and that it was time for the U.S. government to act and restore the trust of their customers around the world (The Guardian, 2013). And Cisco CEO John Chambers warned President Barack Obama of a “collapse of trust in U.S. technology” (D. Thomas & Waters, 2014, p. 1). In the following weeks and months after the first revelations of the NSA surveillance activities, several U.S. internet companies such as Facebook, Microsoft (McCullagh, 2013), Google (Google, 2013a) and Yahoo (M. Mayer & Bell, 2013) started to publish statistics about national security requests and demanded to be allowed to publish more detailed figures (Carroll, 2013).

One of the most prominent responses of the U.S. technology industry was an initiative named Reform Governance Surveillance which included some of the most influential U.S. internet companies including Apple, Facebook, Google and Microsoft (Reform Government Surveillance, 2013). In December 2013, in reaction to the NSA global surveillance activities, the group wrote a joint open letter to the president of the United States and the members of congress with a formal request to reform the U.S. government surveillance practices. Two years later, in May 2015, the companies wrote a second letter urging the members of the U.S. senate to pass the USA Freedom Act to prevent the bulk collection of internet metadata and to increase transparency about government demands for user information (Nakashima, 2015).

Despite the decision by the United States Court of Appeals and recent changes to the U.S. legislation such as the USA Freedom Act of 2015, the U.S. cloud providers apparently still see a great necessity for the U.S. government to change the current law. In a recent example, Microsoft, backed by other U.S. companies (Volz, 2016), sued the U.S. government over the frequent use of secrecy orders that prevent cloud providers to inform their customers when the government obtains a warrant to access their data (J. Greene & Barrett, 2016). A few months earlier, Apple, supported by several U.S. technology companies (Pettersson, 2016), rejected to break into an Apple smartphone that was confiscated by the FBI (Apple, 2016).

Having discussed how U.S. cloud providers reacted to the NSA global surveillance, the following section will review the reactions of the cloud providers in Germany.

2.3.4 German cloud provider reactions

While U.S. cloud providers reportedly presumably experienced a negative impact because of the NSA surveillance programme discussions, non-U.S. cloud providers might, on the other hand, have benefited from the surveillance scandals (Kerkmann, 2013a; Techconsult, 2013c). For example, Switzerland's largest cloud provider Artmotion reported an increase in revenue of 45% a few weeks after the first disclosures of the NSA PRISM programme (Taylor, 2013). Likewise, the customer base of a Norwegian email service increased by 34% after the publications of the Snowden documents (Miller, 2014).

Hence, the "significant erosion in trust" in U.S. public cloud computing service providers (R. Greene et al., 2014, p. 5) might have created a new market for European public cloud computing services companies (J. Baker, 2011) that actively promoted that their customer's data was safe from the USA PATRIOT Act (Hackmann, 2012). IT practitioner publications reported that German cloud providers were actively "fuelling" the debate about the USA PATRIOT Act in order to use the situation for their own benefit (Experton, 2012, p. 7) and that German public cloud service providers were using the NSA surveillance scandal to market their own data centre solutions (Hackmann, 2013; Haffa, 2013).

However, the trend of so-called "data localisation", which is the attempt to keep data and servers in the country, was not new (Hill, 2014). Already in 2010, before the public discussions around the USA PATRIOT Act started, BITKOM, Germany's largest information and communication technology association, expressed their wish for a "German Cloud" (Hackmann, 2010). Nevertheless, the revelations around the U.S. law enforcement practices apparently increased this demand (Scott, 2014a). It seems that after the NSA PRISM disclosures it was even easier for politicians and companies outside the U.S. to make the case for a national cloud scenario (Castro, 2013).

The most prominent example in Germany might be T-Systems, the IT division of Deutsche Telekom (Computerwoche, 2012; Martucci et al., 2012; Meyer, 2013). Long before the U.S. surveillance scandals, T-Systems has been one of the "most vocal and active telecom operators on network security and data privacy issues" (Donegan, 2014) and was possibly trying to convince German and European companies to host their data in the data centres of T-Systems (Rahn, 2011) by stressing the fact that

neither international nor national government organisations have direct access to any customer data (Hackmann, 2013). However, also smaller cloud services providers like PIRONET NDH pointed towards the USA PATRIOT Act and recommend to use a public cloud service provider in Germany or in the EU (Business-Cloud, 2011).

Cloud providers from other European countries might have also used the public awareness of the U.S. surveillance programmes to their own advantage. F-Secure, a Finnish cloud storage and security company, stated that cloud services are “very much about trust” and that their geographical location in Europe helps the company to differentiate itself, “particularly against U.S. companies” (Scott, 2014a, p. 1). The Cyber Security Advisor for France Telecom-Orange, Jean-François Audenard said in an interview that it was not good for the future of European citizens if all data of European companies was under the control of the U.S. and that it was extremely important that European governments were taking care of this issue (Rahn, 2012). The Security and Justice Minister of the Netherlands told the parliament that U.S. companies would be excluded from future IT services contracts because of fears that data could be compromised (Rahn, 2012). In addition, the French government is financially supporting two cloud computing joint ventures which both promise to keep customer data in France (Sayer, 2012; Telecompaper, 2012a, 2012b).

U.S. companies such as IBM have already expressed their concerns that these government interventions would distort competition in France and other countries (Gueugneau, 2012). Additionally, several U.S. press reports claimed that European governments decided “not to lose another technology battle to the U.S.” (Rahn, 2012) and therefore started a “cynical campaign against U.S. cloud providers” (Linthicum, 2012, p. 1) by implementing some kind of “cloud protectionism” (Darrow, 2012, p. 1). According to the authors, the EU was using “fear, uncertainty and doubt” to keep IT investments in Europe (Linthicum, 2012, p. 1) and the NSA scandal would “provide more fuel for the already cloud-paranoid” (Linthicum, 2013, p. 1). U.S. President Barack Obama commented that “sometimes the European response here is more commercially driven than anything else” and that European cloud providers were “trying to set up some roadblocks” for U.S. companies (Swisher, 2015, p. 10).

However, even if the data localisation initiatives of local governments in Europe and other countries outside the U.S. were mostly opportunistic (Hill, 2014), the NSA global

surveillance disclosures most probably had a direct negative impact on the competitiveness of U.S. cloud providers and their business in Europe (Donohue, 2015). Therefore, it should be in the own interest of the U.S. cloud providers to improve the trust relationships with their current and potential clients to counteract possible negative monetary consequences. One of the objectives of the current research is to identify ways how U.S. cloud providers can improve the trust relationship with German companies.

2.4 Summary

Cloud computing technologies hold immense potential for German companies. The most business benefits can be achieved with the public cloud computing deployment model. Currently, the most advanced public cloud services for enterprise customers are offered by U.S. cloud providers, such as Amazon, Google and Microsoft.

Already before the revelations of the global surveillance programmes of U.S. intelligence agencies, German companies had a relatively low adoption rate of public cloud computing services in comparison with other countries in the world and in Europe. The main concerns raised by German companies were about cloud computing security, cloud computing privacy and about legal aspects.

However, the news around the NSA global surveillance activities have further reinforced these concerns. Political leaders of the EU and Germany openly addressed the loss of trust in the U.S. government and the consequential repercussions for cloud computing adoption. German politicians called for a boycott of U.S. technology companies, more stringent data privacy requirements and for private European data networks.

Several international surveys indicated that, because of the global surveillance programmes, German companies preferred to keep their data in their own data centres, avoided U.S.-based cloud providers and did not trust the U.S. to play an important role in running global Internet services.

The NSA surveillance scandal had probably a negative impact on the U.S. economy and on the business of U.S. cloud providers. Market analysts predicted that the public awareness of the NSA programmes would cost U.S. cloud providers billions of dollars in lost sales and in investments in data centres abroad. Faced with the choice between

complying with secret government requests and maintaining the trust of their customers, U.S. cloud providers decided to promote legislative changes and take legal action against the U.S. government.

German cloud providers and their European counterparts might have seen sales and revenue increases from the discussions around the global surveillance disclosures. Some of them were actively promoting that their cloud services are protected against unjustified access by U.S. intelligence agencies. Additionally, European governments were financially supporting local cloud service providers.

The responses of government officials, German companies, U.S. cloud providers and German cloud providers show that the notion of trust plays a significant role in cloud computing business. The following literature review will therefore further explore the concept of trust in buyer-seller relationships in general and more particularly in cloud computing business relations.

3 Literature review

The purpose of this chapter is to review the body of literature relevant to the objectives of this research with a focus on the notion of trust. Trust is a broad and complex concept which can be analysed from very different angles. Due to practical constraints, this chapter cannot provide a comprehensive review of all aspects of trust. Nevertheless, it is important to have a mutual understanding of the basic principles and definition of trust in a buyer-seller relationship context. The literature review chapter is structured in the following way (see Figure 11).

The first section will highlight the importance of the concept of trust for the human society in general and for business relationships in particular. Section 3.2 will give an overview of the different definitions of trust by philosophers, sociologists and economists. The following sections will review the literature on trust in buyer-seller relationships and focus on the trust relationships between the buyer and the selling company, the buyer and the salesperson and the buyer and the product or service.

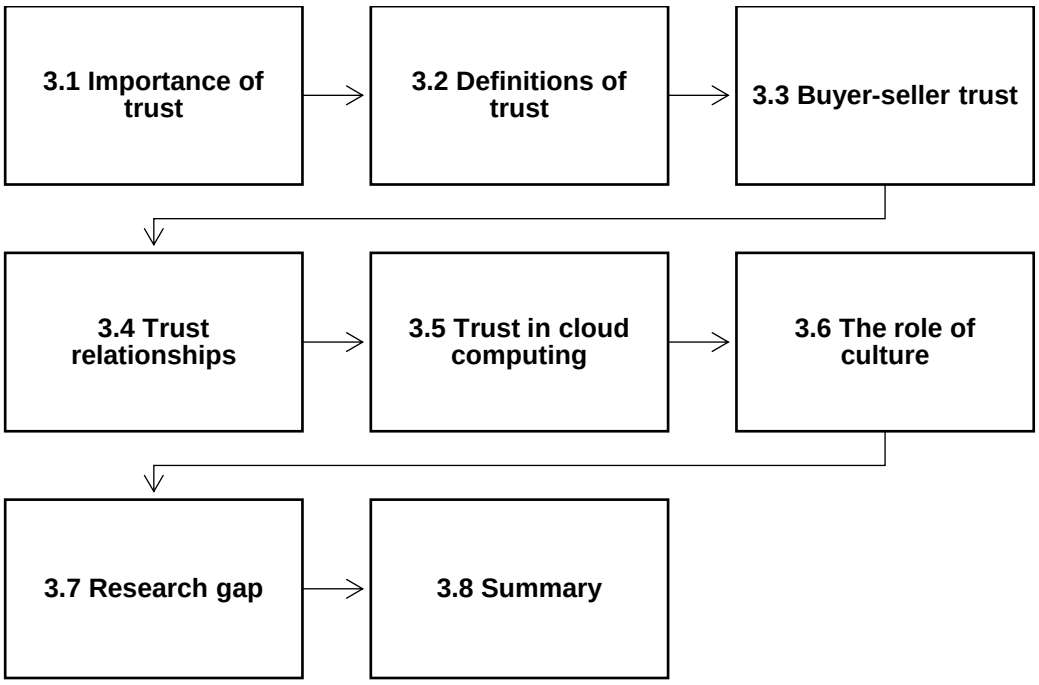


Figure 11: Literature review chapter

In addition, Section 3.5 will discuss the present literature on trust in cloud computing services. The following section deals with the interplay between culture and trust and the characteristics of the U.S. and German culture.

The subsequent section addresses the gaps in the knowledge based on the reviewed literature and formulates the research questions for the current study. Finally, the last section summarises the literature review chapter.

3.1 Importance of trust

There is a consensus among philosophers, sociologists and economists on the importance of the concept of trust for humankind (Hosmer, 1995). As discussed in the following section on the definition of trust, the concept of trust may be as old as humanity itself and literature on the importance of trust dates back several decades. From a philosophical viewpoint, “trust is a social good to be protected just as much as the air we breathe” and “when it is destroyed, societies falter and collapse” (Bok, 1979, p. 28).

Sociologists describe trust as vital to the understanding of social life (Deutsch, 1958), a necessity for stable social relations (Blau, 1964), a fundamental component of human actions (Sztompka, 1999) and as a central determinant of behaviour (Rotter, Chance, & Phares, 1972). Based on Gibb’s (1964) theory of group development, Friedlander (1970) found that trust between members of a group leads to higher effectiveness of that group. According to Golembiewski and McConkie (1975, p. 131) there is perhaps “no single variable which so thoroughly influences interpersonal and group behaviour as does trust”. Other authors described trust as the “basis of all human systems of morality” (Nowak & Sigmund, 2000, p. 819), as the foundation of society and civilisation (Putnam, 2000) and as key to human happiness (Haidt, 2006; Layard, 2011).

Luhmann, Davis, Raffan, and Rooney (1979, p. 4) went even further by declaring that the only alternative to trust is “chaos and paralysing fear”. Whether it is about lending money, forming a community or visiting a doctor, “interpersonal trust is a basic feature of all social situations that demand cooperation and interdependence” (Johnson-George & Swap, 1982, p. 1306). Barber (1983, p. 21) reemphasized the critical importance of trust in interpersonal and group behaviour as an “integrative mechanism that creates and sustains solidarity in social relationships and systems”, which has been backed up by Butler (1991, p. 647), who characterised trust as an “important aspect of interpersonal relationships”. Lewis and Weigert (1985a, p. 456) even went

that far to say that “trust is a functional necessity for society”. Likewise, according to Seligman (2000), any social order must be based on mutual trust between the actors.

Economists claimed that “commodity exchange […] is possible only on the basis of far-reaching personal confidence and trust” (Weber, 1968, p. 114). The level of trust inherent in a society is a critical factor for “a nation’s well-being, as well as its ability to compete” (Fukuyama, 1995, p. 7). In an experiment with business executives, Zand (1972) found that managerial problem solving effectiveness is significantly higher in high-trust groups than in low-trust environments. Other studies found that mutual trust is “the cornerstone to the strategic partnership“ (Spekman, 1988, p. 79) and business relations that are based on personal trust survive greater stress and can better adapt to new circumstances (Williamson, 1979).

Trust was also found to have an important impact on the stability of long-term business relationships (E. Anderson & Weitz, 1989; Ganesan, 1994; Ryu, Park, & Min, 2007; Zhao & Tamer Cavusgil, 2006), is a “crucial element in social exchange processes” (Hailén, Johanson, & Seyed-Mohamed, 1991, p. 31), a “precondition of social life” (Sabel, 1993, p. 1136), improves business performance (Sako, 1998), reduces conflicts (A. Zaheer, McEvily, & Perrone, 1998), improves supply chain performance (Kwon & Suh, 2004, 2005), increases cooperation (Johnston, McCutcheon, Stuart, & Kerwood, 2004), improves supplier responsiveness (Handfield & Bechtel, 2002), increases (re-) purchase intentions (Gurun, Stoffman, & Yonker, 2017; Hewett, Money, & Sharma, 2002), supports innovation (Lewan, 2018; Zhu, Habisch, & Thøgersen, 2018) and is a “key to successful international alliances” (Parkhe, 1998a, p. 417).

In business exchange relationships, trust reduces the perception of risk, increases confidence and reduces transactional costs (Ganesan, 1994). Trust is also viewed as an essential concept by business practitioners, who all stressed the critical importance of trust within and between organisations (e.g. Lewis (2007) and Shaw (1997)).

Lack of trust, on the other hand, reduces the rate of investments (Zak & Knack, 2001), decreases the amount of trade (Braynov & Sandholm, 2002) and is a main reason for failed business alliances (Parkhe, 1998b). In the absence of trust, it is unlikely that business partners share proprietary information (Cannon & Perreault Jr, 1999; Gill & Crane, 2017). Furthermore, when trust is low between companies, they are more likely to spend time and money on monitoring and analysing each other’s behaviour to

protect themselves against the partner's opportunism (Geyskens, Steenkamp, Scheer, & Kumar, 1996; Sitkin & Roth, 1993).

Despite this mutual agreement on the importance of trust, there seems to be an equally widespread disagreement on a common definition of the concept (Hosmer, 1995). Before proceeding to examine the literature on trust in buyer-seller relationships, it will therefore be necessary to review the different definitions and find an appropriate characterisation of trust for this study.

3.2 Definitions of trust

There is no single universally accepted definition of trust (Audi, Loughran, & McDonald, 2016) and "every discipline views trust from its own unique perspective" (D. Harrison McKnight & Chervany, 2001, p. 37). But even within one scientific discipline such as sociology, the characterisations and definitions of trust differ widely. As Plank, Reid, and Ellen Bolman (1999) argued, "there is no true consensus on a definition of trust nor any accepted cross-disciplinary paradigm". Husted (1989, p. 23) explained that "the definition of trust is problematic because there is such a wide variety of approaches to the concept".

It is therefore important to understand how the different disciplines characterised this concept and not only focus on the definition of trust by economics. This broad variety of definitions of trust inside one discipline and across disciplines shows that it can be challenging to study and measure trust if there is no consent about what trust actually is and how it can be defined. The following sections will hence discuss the various definitions of trust by philosophers, sociologists and economists and select a trust definition for this study.

3.2.1 Definitions of trust by philosophers

Although moral philosophers always had a strong interest in cooperation between people, they paid surprisingly little attention to the concept of trust (Baier, 1986). The "classical ethicists –Socrates, Plato, Aristotle, St. Augustine, St. Thomas Aquinas, Hobbes, Locke, Rousseau, Mill, Kant. Smith, Jefferson, Ross, Rawls, and Nozic – scarcely mention the term" (Hosmer, 1995, p. 394) while discussing friendship, cooperation and related concepts of the human being (Blomqvist, 1997). Hosmer (1995) also pointed out, that only a fraction of the articles in the Encyclopaedia of

Ethics (1992) discuss the topic of trust and only include minor citations from philosophers such as Aristotle and Locke. According to Hosmer (1995, p. 394), this "strange silence" on the topic might be explained with the tradition and goal of Western moral philosophy to find the "ideal rule" instead of analysing the human behaviour resulting from the use of that rule.

However, there are some characteristics of trust which have been given more attention by the great philosophers. Saint Thomas Aquinas praised the ideas of faith, hope and the trust in God, while John Locke was more passionate about trust in governments, officials and contracts (Baier, 1986). According to Hobbes (1650), who provided one of the first definitions of trust, a person that trusts does not set up any safeguards (Blomqvist, 1997). Baier (1986, p. 234) stated that there are different forms of reliance on persons, whereof trust is the "reliance on another's good will". The idea of the "good will" is also the central concept of Kant's Groundwork for the Metaphysics of Morals (Hosmer, 1995), in which he contends that "nothing can possibly be conceived in the world, or even out of it, which can be called good without qualification, except a good will" (Kant, 2005, p. 55). Instead of formulating an additional definition of trust, Lagerspetz (1998, p. 4) argued that it was "neither realistic nor helpful to look for a definition of trust in terms of sufficient and necessary conditions" and proposed to look at different circumstances in which the word is used (Lahno, 1999). Table 13 provides an overview of key definitions of trust by philosophers.

Table 13: Summary of key definitions of trust by philosophers

Author(s)	Definition
Hobbes (1650, p. 8)	"Trust is a passion proceeding from the belief of him from whom we expect or hope for good, so free from doubt that upon the same we pursue no other way to attain the same good: as distrust or diffidence is doubt, that makes him endeavour to provide himself other means."
Baier (1986, pp. 234, 235, 259)	"Trust … is reliance on another's good will." "Trust … is accepted vulnerability to another's possible but not expected ill will (or lack of good will) toward one. "Trust … is reliance on others' competence and willingness to look after, rather than harm, things one cares about which are entrusted to their care."
Hertzberg (1988)	"Trusting another person means having a trusting attitude towards the other person, without specifying where he is trusted, as could be said that after judgement somebody is relied in upon certain aspects. Trust thus is implicit, not placed on grounds and never a rational option."

Other philosophers answered the question why we trust with "because we have to" (Pirson, 2007). According to Socrates, "no individual is self-sufficient and every

individual must therefore cooperate with those who can supply his needs in return for his contributing to theirs" (Sofroniou, 2007, p. 73). And since the information we have about others is incomplete (Bachmann & Zaheer, 2006), we do not have a choice but to trust them. Similarly, Hollis (1998, p. 1) concluded that "everyday life is a catalogue of success in the exercise of trust".

Having discussed how philosophers define trust, the following section will outline how the social sciences approach this concept.

3.2.2 Definitions of trust by sociologists

An early sociological discussion on trust was undertaken in the 1950s and 1960s by sociologists such as Mellinger (1956), Deutsch (1958), Blau (1964), Giffin (1967) and Rotter (1967). While Deutsch (1958) concentrated on the motivational aspects of a trusting relationship, Blau (1964) stressed the social aspects of the concept. Giffin (1967) and Rotter (1967), on the other hand, highlighted the dependence on the intention of an individual or group.

In the 1970s, sociologists as for instance Schlenker, Helm, and Tedeschi (1973), Lindskold and Bennett (1973) and Frost, Stimpson, and Maughan (1978) combined those early definitions and highlighted the importance of the concept of risk, reliance and uncertainty to the notion of trust. Their definitions are based on an unclear situation that may lead to a positive or negative outcome, a certain dependence of the trusting person on another person and a confidence in the unselfishness of the trusted person.

At the beginning of the 1980s, however, the books of Luhmann et al. (1979) on "Trust and power" and Barber (1983) on "The logic and limits of trust"' have "placed trust at the centre of sociological theorizing about contemporary society" (Lewis & Weigert, 1985b). Luhmann et al. (1979, p. 8) complained about the situation that, although trust was a key mechanism in social life, there was a "regrettably sparse literature which has trust as its main theme within sociology".

Barber (1983, p. 7) agreed with Luhmann et al. (1979) by saying that "in both serious social thought and everyday discourse", it was "assumed that the meaning of trust, and of its many apparent synonyms, is so well known that it can be left undefined or to contextual implications". Drawing on the work of Luhmann et al. (1979) and Barber

(1983), Lewis and Weigert (1985b, p. 967) agreed that although there was a large quantity of research on trust in psychology and politics, the literature appeared, however, “theoretically unintegrated and incomplete from the standpoint of a sociology of trust”.

As shown in Table 14, most sociologists used the term “expectation” (Bradach & Eccles, 1989; Deutsch, 1958; Frost et al., 1978; Lewis & Weigert, 1985b; Rotter, 1967; Uslaner, 2002) in their definition of trust. Their definitions are based on the concept that one party expects a certain action or behaviour from the other party. Other authors called it “belief” (Larzelere & Huston, 1980), “desire” (Giffin, 1967) or “subjective probability” (Gambetta, 1988). Some definitions went one step further by including the idea of “reliance or dependence” (Giffin, 1967; Rotter, 1967; Schlenker et al., 1973) upon the behaviour of a person or group, the characteristics of an object or the occurrence of an event.

Table 14: Definitions of trust by sociologists.

Author(s)	Definition
Deutsch (1958, p. 266)	“An individual may be said to have trust in the occurrence of an event if he expects its occurrence and his expectation leads to behaviour which he perceives to have greater negative motivational consequences if the expectation is not confirmed than positive motivational consequences if it is confirmed.”
Blau (1964, p. 315)	"The process of social exchange …generates trust in social relations.”
Giffin (1967, p. 105)	"Interpersonal trust may be defined as a reliance upon the characteristics of an object, or the occurrence of an event, or the behaviour of a person in order to achieve a desired but uncertain objective in a risky situation."
Rotter (1967, p. 651)	"Interpersonal trust is defined here as an expectancy held by an individual or a group that the word, promise, verbal or written statement of another individual or group can be relied upon."
Schlenker et al. (1973, p. 419)	"Reliance upon information received from another person about uncertain environmental states and their accompanying outcomes in a risky situation."
Frost et al. (1978, p. 104)	"An expectancy held by an individual that the behaviour (verbal or nonverbal) of another individual or group of individuals would be altruistic and personally beneficial to himself."
Larzelere and Huston (1980, p. 595)	“Trust is most generally defined as a belief by a person in the integrity of another individual.”
Lewis and Weigert (1985b, pp. 968, 971)	“Therefore, we may say that trust exists in a social system insofar as the members of a system act according to and are secure in the expected futures constituted by the presence of each other for their symbolic representations.” “The behavioural content of trust is the undertaking of a risky course of action on the confident expectation that all persons involved in the action will act competently and dutifully.”
Zucker (1986, p. 54)	“From a sociological perspective, trust is defined as a set of expectations shared by all those involved in an exchange.”
Gambetta (1988, p. 217)	“Trust (or, symmetrically, distrust) is a particular level of the subjective probability with which an agent assesses that another agent or group of agents will perform a particular action, both before he can monitor such action (or independently of

	his capacity ever to be able to monitor it) and in a context in which it affects his own action."
Good (1988, p. 33)	"Trust is based on an individual's theory as to how another person will perform on some future occasion, as a function of that target person's current and previous claims, either implicit or explicit, as to how they will behave."
Bradach and Eccles (1989, p. 104)	"Trust is a type of expectation that alleviates the fear that one's exchange partner will act opportunistically."
Uslaner (2002, p. 2)	"When we trust other people, we expect that they will fulfil their promises, either because we know that they have usually done so in the past or because we believe that we shall fare better if we presume that others are trustworthy."

Another important element in many definitions is that of an "uncertain environmental state" (Giffin, 1967; Schlenker et al., 1973) or a "risky situation" (Giffin, 1967; Lewis & Weigert, 1985a; Schlenker et al., 1973) that can have "negative consequences" (Deutsch, 1958) for the trusting person. Schlenker et al. (1973) even claimed that trust could not be demonstrated if any of these elements was lacking.

The definition of trust by the sociologists had a strong influence on the definition of trust by the economists, which will be demonstrated in the following section.

3.2.3 Definitions of trust by economists

According to Moorman, Zaltman, and Deshpande (1992), there are two general approaches to trust in the economics literature. One aspect of trust is based on the definition of sociologists like Blau (1964) and Rotter (1967), that trust is a "belief, sentiment, or expectation" about the trustworthiness of another person, as a result of that person's "expertise, reliability, or intentionality".

For example, Schurr and Ozanne (1985, p. 940), who have been influential for most economists literature on trust (Blois, 1999), based their definition on the work of Blau (1964) and Rotter (1967), and defined trust as "the belief that a party's word or promise is reliable and that a party will fulfil his/her obligations in an exchange relationship".

Moorman et al. (1992, p. 315) also based their work on the classic view of Rotter (1967) and argued that both belief and behavioural intention must be present for trust to exist (Blomqvist, 1997). They claimed that if someone was willing to rely on another person without believing in the trustworthiness of that person, this may rather indicate a relationship of power and control than of trust (Moorman, Deshpande, & Zaltman, 1993). The definition of Morgan and Hunt (1994) parallels the description of (Moorman et al., 1993); Moorman et al. (1992) and equally highlights the importance of

confidence which results from the belief that the other party is reliable, competent, fair, honest, responsible, helpful and has integrity.

Other economists such as Sako (1992) and Doney and Cannon (1997) also based their definition on the expectation that the written statement or word of the exchange partner can be relied on. Table 15 provides an overview of the general approaches to trust in the economics literature.

Table 15: Summary of key definitions of trust by economists

Author(s)	Definition
Zand (1972, p. 230)	“Trusting behaviour … is defined here as consisting of actions that (a) increase one's vulnerability, (b) to another whose behaviour is not under one's control, (c) in a situation in which the penalty (disutility) one suffers if the other abuses that vulnerability is greater than the benefit (utility) one gains if the other does not abuse that vulnerability.”
Bialaszewski and Giallourakis (1985, p. 207)	“Trust has been defined as an attitude displayed in situations where the following characteristics may be evident: a person is relying on another person, a person is risking something of value, and/or a person is-attempting to achieve a desired goal.”
Schurr and Ozanne (1985, p. 940)	“Trust has been defined as the belief that a party's word or promise is reliable and that a party will fulfil his/her obligations in an exchange relationship.”
Lorenz (1988, p. 197)	“Trusting behaviour consists in action that (1) increases one’s vulnerability to another whose behaviour is not under one’s control, and (2) takes place in a situation where the penalty suffered if the trust is abused would lead one to regret the action.”
Zaltman and Moorman (1988, p. 17)	“Drawing upon both the research literature and our interviews, we define trust as an interpersonal or interorganizational state that reflects the extent to which the parties can predict one another’s behaviour; can depend on one another when it counts; and have faith that the other will continue to act in a responsive manner despite an uncertain future.”
E. Anderson and Weitz (1989, p. 312)	"We define trust as one party's belief that its needs will be fulfilled in the future by actions undertaken by the other party."
J. C. Anderson and Narus (1990, p. 45)	"Trust in a working relationship and its implications for a firm’s actions have been defined as the firm's belief that another company will perform actions that will result in positive outcomes for the firm as well as not take unexpected actions that result in negative outcomes for the firm."
Morgan (1991, p. 92)	“Trust has been conceptualized for the present study as the belief that another party: (a) will not act in a way that is harmful to the trusting firm; (b) will act in such a way that is beneficial to the trusting firm; and (c) will act reliably.”
Moorman et al. (1992, p. 315), Moorman et al. (1993, p. 82)	“Trust is defined as a willingness to rely on an exchange partner in whom one has confidence.”
Sako (1992, p. 37)	“Trust is a state of mind, an expectation held by one trading partner about another, that the other behaves or responds in a predictable and mutually acceptable manner.”
Sabel (1993, p. 1133)	“Trust, the mutual confidence that no party to an exchange will exploit the other's vulnerability, …”
Sitkin and Roth (1993)	“A belief, attitude, or expectation concerning the likelihood that the actions or outcomes of another individual, group or organization will be acceptable or will serve the actor's interests.”

Barney and Hansen (1994, p. 176)	“Trust is the mutual confidence that no party to an exchange will exploit another's vulnerabilities.” See Sabel (1993)
Morgan and Hunt (1994, p. 23)	“We conceptualize trust as existing when one party has confidence in an exchange partner’s reliability and integrity.”
Fukuyama (1995, p. 26)	“Trust is the expectation that arises within a community of regular, honest, and cooperative behaviour, based on commonly shared norms, on the part of other members of that community.”
Hosmer (1995, p. 399)	“Trust is the expectation by one person, group, or firm of ethically justifiable behaviour -- that is, morally correct decisions and actions based upon ethical principles of analysis – on the part of the other person, group, or firm in a joint endeavour or economic exchange.”
Madhok (1995, p. 120)	“Trust is the perceived likelihood of the other not behaving in a self-interested manner.”
R. C. Mayer, Davis, and Schoorman (1995, p. 726)	“In sum, trust is a willingness to be vulnerable to another party, but there is no risk involved with holding such an attitude.”
McAllister (1995, p. 25)	“Combining these ideas yields a definition of interpersonal trust as the extent to which a person is confident in, and willing to act on the basis of, the words, actions, and decisions of another.”
Robinson (1996, p. 576)	“Trust is defined here as one’s expectations, assumptions, or beliefs about the likelihood that another's future actions will be beneficial, favourable, or at least not detrimental to one's interests.”
Doney and Cannon (1997, p. 36)	“We define trust as the perceived credibility and benevolence of a target of trust.”
Lorenz (1999, p. 305)	“Trust can be defined as the judgement one makes on the basis of one's past interactions with others that they will seek to act in ways that favour one's interests, rather than harm them, in circumstances that remain to be defined.”
Plank et al. (1999, p. 62)	“Trust is a global belief on the part of the buyer that the salesperson, product and company will fulfil their obligations as understood by the buyer.”
James Jr (2002, p. 291)	“Trust can be viewed as an expectation, and it pertains to circumstances in which agents take risky actions in environments characterized by uncertainty or informational incompleteness.”
Nooteboom (2002, pp. 45,48)	Definition 1: “Trust in things or people entails the willingness to submit to the risk that they may fail us, with the expectation that they will not, or the neglect or lack of awareness of the possibility that they might.” Definition 2: “'Real' trust, or trust in the strong sense, is an expectation that things or people will not fail us, or the neglect or lack of awareness of the possibility of failure, even if there are perceived opportunities and incentives for it.”
Sobel (2002, p. 148)	“Trust is the willingness to permit the decisions of others to influence your welfare.”

The second aspect of trust is based on the definition of sociologists like Deutsch (1958), Giffin (1967) and Schlenker et al. (1973), which includes a reliance on the other party and implies that trust is unnecessary without uncertainty, risk and vulnerability (Moorman et al., 1992). According to the sociologists Johnson-George and Swap (1982, p. 1306), the “willingness to take risks may be one of the few characteristics common to all trust situations”. Some of the following definitions, however, are a combination of both approaches.

Following Deutsch (1958), Zand (1972, p. 230) defined trusting behaviour as “consisting of actions that (a) increase one's vulnerability, (b) to another whose behaviour is not under one's control, (c) in a situation in which the penalty (disutility) one suffers if the other abuses that vulnerability is greater than the benefit (utility) one gains if the other does not abuse that vulnerability”. The results of his study indicate that individuals in high-trust environments are significantly more effective in problem solving than those who work in low-trust environments. The findings of Boss (1978) add additional support to the conclusions of Zand (1972) and show that the degree to which one party trusts the other party defines the grade to which they share important information and let them influence their decisions.

The definitions of trust by Bialaszewski and Giallourakis (1985), Lorenz (1988) and Zaltman and Moorman (1988) are also based on the second aspect of trust. Bialaszewski and Giallourakis (1985) followed the view of (Giffin, 1967) and argued that, in a trust relationship, a person must be risking something of value. Lorenz (1988, p. 197) included in his definition that trusting behaviour consists in action that “takes place in a situation where the penalty suffered if the trust is abused would lead one to regret the action”. The definition by Zaltman and Moorman (1988) is based on the concept of embeddedness of Shapiro (1987), that trust is built on the incremental increase of well elaborated and timed actions of both parties in a relationship.

Following the definition used by Pruitt (1981), E. Anderson and Weitz (1989, p. 312) defined trust as “one party's belief that its needs will be fulfilled in the future by actions undertaken by the other party”. Although they did not mention any uncertainty, risk or vulnerability in their definition of trust, they acknowledged in their study that one party must rely on the other party and that any type of coordinative behaviour leaves both parties open to exploitation (E. Anderson & Weitz, 1989).

The definition of J. C. Anderson and Narus (1990) focused on the perceived outcomes of trust (Morgan & Hunt, 1994) and, more specifically, on the relationship between the working partnership between distributor firms and manufacturer firms. They added that trust can be maintained even if one party did not fulfil their part of an agreement. This may be the case if the company believes that its partner had taken the agreed actions but that some forces beyond the control of the partner have led to a different result.

Sabel (1993, p. 1133) also focused on the risk aspects in economic relations and claimed that, without trust, none of the parties would risk moving first and thereby miss the gains of cooperation in favour of a less lucrative pursuit of egoism. According to R. C. Mayer et al. (1995), trust, is not per se taking risk, but rather the willingness to make oneself vulnerable. More recent definitions, e.g. Plank et al. (1999) and Nooteboom (2002), extended the definition of trust to also include „things“ such as products and services (see Section 3.3.2). Recent literature on trust is referring to the definitions presented in Table 15. It could therefore be argued that the definitions created in the last decades are still relevant and that newer studies did not create any additional definitions.

Based on the verbalisation of the concept of trust reviewed above, the following section will determine a definition of trust for this study.

3.2.4 Definitions of trust for this study

In their cross-discipline view of trust, Rousseau, Sitkin, Burt, and Camerer (1998, p. 394) concluded, that there is “no universally accepted scholarly definition of trust”. However, the authors found a “considerable overlap and synthesis in contemporary scholarship on trust” (Rousseau et al., 1998, p. 402) and suggested to define trust as “a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behaviour of another” Rousseau et al. (1998, p. 395).

Zucker (1986, p. 56), on the other hand, criticized much of the previous work on trust (Hosmer, 1995) and argued that "recognition of the importance of trust has led to concern with defining the concept, but the definitions proposed unfortunately have little in common other than the informal character of trust”. Nevertheless, “the lack of conceptual clarity has not inhibited the wide use of the concept” (Bluhm, 1987, p. 334).

Since the current study is conducted in the field of marketing science, the definitions of trust by economists appear to be the most suitable choice for the context of this research. Therefore, trust in this study is defined as the expectation that the other party will fulfil their obligations and the mutual confidence, that no party to an exchange will exploit another's vulnerabilities.

Having defined what is meant by trust in the context of this study, the following sections will review the literature on trust between buyers and sellers.

3.3 Buyer-seller trust

In their early work about behaviour in organisations, L. W. Porter, Lawler, and Hackman (1975, p. 497) stated that although trust was “widely assumed to be good for organisations”, there was not much research about what that actually “means in an organisational context”. However, the discussion of trust as an important variable for buyer-seller relationships in business to business (B2B) markets has increased in the following decades (Blois, 1999; Y. Huang & Wilkinson, 2013; Sako, 1998; Young & Wilkinson, 1989). The changing dynamics of today’s global marketplace requires companies to be effective co-operators and to develop professional networks based on commitment and trust (Morgan & Hunt, 1994). And even though the process of building buyer trust is complex, time-consuming and costly, the outcome in terms of stronger relationship bonds and greater loyalty can be vital to the seller companies (Doney & Cannon, 1997).

Buyer-seller trust is a complex concept and researchers choose different theoretical methods to capture its nature (Blomqvist, 2002; Hernandez & dos Santos, 2010; Xu, Cenfetelli, & Aquino, 2016). For example, Seppänen, Blomqvist, and Sundqvist (2007) found over twenty different dimensions of trust, whereof reliability (e.g., Aulakh, Kotabe, & Sahay, 1996; Chow & Holden, 1997; Coote, Forrest, & Tam, 2003; Dyer & Chu, 2000; J. B. Smith & Barclay, 1997; A. Zaheer et al., 1998) and credibility/competence (e.g., Doney & Cannon, 1997; Ganesan, 1994; Norman, 2002; Sako & Helper, 1998) were the most common ones.

Other studies focused on the antecedents and consequences of trust in different settings such as in global business (e.g., Sirkka L. Jarvenpaa, Knoll, & Leidner, 1998; Tat Koon Koh, Mark Fichman, & Robert E Kraut, 2012), in management (e.g., Bijlsma & Van De Bunt, 2003; Mahajan, Bishop, & Scott, 2012; Whitener, Brodt, Korsgaard, & Jon, 1998), in buyer-seller interaction (Celuch, Bantham, & Kasouf, 2011; Doney & Cannon, 1997; e.g., Gulati & Sytch, 2008); D. Johnson and Grayson (2005); (Selnes, 1998) and in online business (Beldad, de Jong, & Steehouder, 2010; e.g., Bijlsma & Van De Bunt, 2003; Chiu, Hsu, Lai, & Chang, 2012; e.g., Chiu, Huang, & Yen, 2010; McCole, Ramsey, & Williams, 2010; Sung-Joon, 2002; Whitener et al., 1998). One

example of an antecedent of trust is liking (e.g. Nicholson, Compeau, and Sethi (2001)) and a consequences of trust can be closeness (e.g. Nielson (1998)). Other researchers, e.g. Schlosser, White, and Lloyd (2006) and Xu et al. (2016), applied the conception of D. Harrison McKnight, Choudhury, and Kacmar (2002) of trusting beliefs (integrity, benevolence, and competence) as the key components of trust.

However, there is no coherent use of the terms. For example, while opportunistic behaviour is consistently seen as having a negative impact on trust, Jiang (2010) found that other concepts such as dependence can be seen as either positively (e.g., Palmatier, Dant, Grewal, & Evans, 2006; Payan & McFarland, 2005) or negatively (e.g., Kumar, Scheer, & Steenkamp, 1995; Young-Ybarra & Wiersema, 1999) related to trust.

Moreover, there is an overlapping and blurred use of vocabulary describing the dimensions, antecedents and consequences of trust and there seems to be no common semantic meaning of those terms (Blomqvist, 1997; Rousseau et al., 1998; Seppänen et al., 2007). For example, some of the consequences of trust, such as commitment, communication and cooperation, can also be found as antecedents of trust. One reason could be that there is no collective agreement on the definition and use of those terms across different studies and disciplines. Another reason may be that trust is a reciprocal concept, which can be both a cause and an effect (Seppänen et al., 2007). For example, Dwyer, Schurr, and Oh (1987) concluded that trust leads to communication, while E. Anderson, Lodish, and Weitz (1987) found that communication causes trust. The interpretation of J. C. Anderson and Narus (1990) of this disagreement is that building and sustaining trust is an iterative process. Consequently, Seppänen et al. (2007) suggest that future research on trust should therefore take into account the reciprocal loops of trust and other concepts such as communication and commitment.

This research will focus on another way to capture the notion of trust in a buyer-seller context, which is by its individual trust relationship. The following two sections will present three distinct types of trust relationships in the buyer-seller relationship literature. The first section will focus on the distinction between the trust of the buyer in the selling company (inter-organisational trust) and the trust of the buyer in the

salesperson of the selling company. The second section will introduce a third type of trust relationship, the trust of the buyer in the product or service.

3.3.1 Inter-organisational and interpersonal trust

In their examination of the nature of trust in buyer-seller relationships, Doney and Cannon (1997) found that most of the existing literature did not differentiate between the trust of a buyer in the selling company and the trust of the buyer in the salesperson of the selling company. Likewise, Ganesan and Hess (1997) claimed that former research did not distinguish between interpersonal trust and organisational trust. Previously, Dwyer et al. (1987) and J. C. Anderson and Narus (1990) suggested that trust in a selling company differs from the trust in the salesperson of the selling company. According to Doney and Cannon (1997), it was particularly important in business marketing to understand the differences between these two trust relationships. However, their review of the existing literature found that most studies of trust in buyer-seller relationships did not explicitly differentiate between the trust of a buyer in the selling company and the trust of the buyer in the salesperson of the selling company.

In fact, Doney and Cannon (1997) only found that the two studies of Swan and Nolan (1985) and Young and Wilkinson (1989) discussed both relationships. A. Zaheer et al. (1998, p. 141) shared this view and stated that “interpersonal and inter-organizational trust are related but distinct constructs”. The authors concluded that, although these constructs were associated with each other, they related differently to parameters such as costs of negotiation. Blois (1999, p. 203) also expressed his concern that “little note has been taken of this problem” and that only Doney and Cannon (1997) and E. Anderson et al. (1987) explicitly addressed the difference between the supplier firm and the salesperson.

Ganesan and Hess (1997) included intra-organisational trust, the trust within organisations, as an additional relationship in their “levels of trust”. However, since the current research concentrates solely on the trust relationships of the buyer with entities outside the buyer’s organisation, intra-organisational trust is not in the scope of this study.

The current research will therefore distinguish between the trust of a buyer in the selling company and the trust of the buyer in the salesperson of the selling company. Sections 3.4.1 and 3.4.2 will review and discuss the most influencing and recent literature on these two trust relationships.

A serious weakness of only involving these two trust relationships is, however, that the trust in the product or service offered by the selling company and the salesperson are not considered. This additional trust relationship will be addressed in the following section.

3.3.2 Individual components of trust

In their exploratory study on trust in business-to-business sales, Plank et al. (1999) claimed that the buyer-seller literature on the object of trust had been rather one-dimensional and mainly focused on interpersonal trust. The authors argued that it was not sufficient to only study the interpersonal trust and the (inter-)organisational trust, but that it was necessary to also consider the expected functions and obligations associated with the offered products and services.

Plank et al. (1999, p. 62) defined these "individual components of trust" as follows:

- *Salesperson trust is the belief that the salesperson will fulfil his/her obligations as understood by the buyer.*
- *Product trust is the belief that the product/service will fulfil its functions as understood by the buyer.*
- *Company trust is the belief that the company will fulfil all its obligations as understood by the buyer.*

Figure 12 displays the components of trust from the perspective of the buyer as defined by Plank et al. (1999).

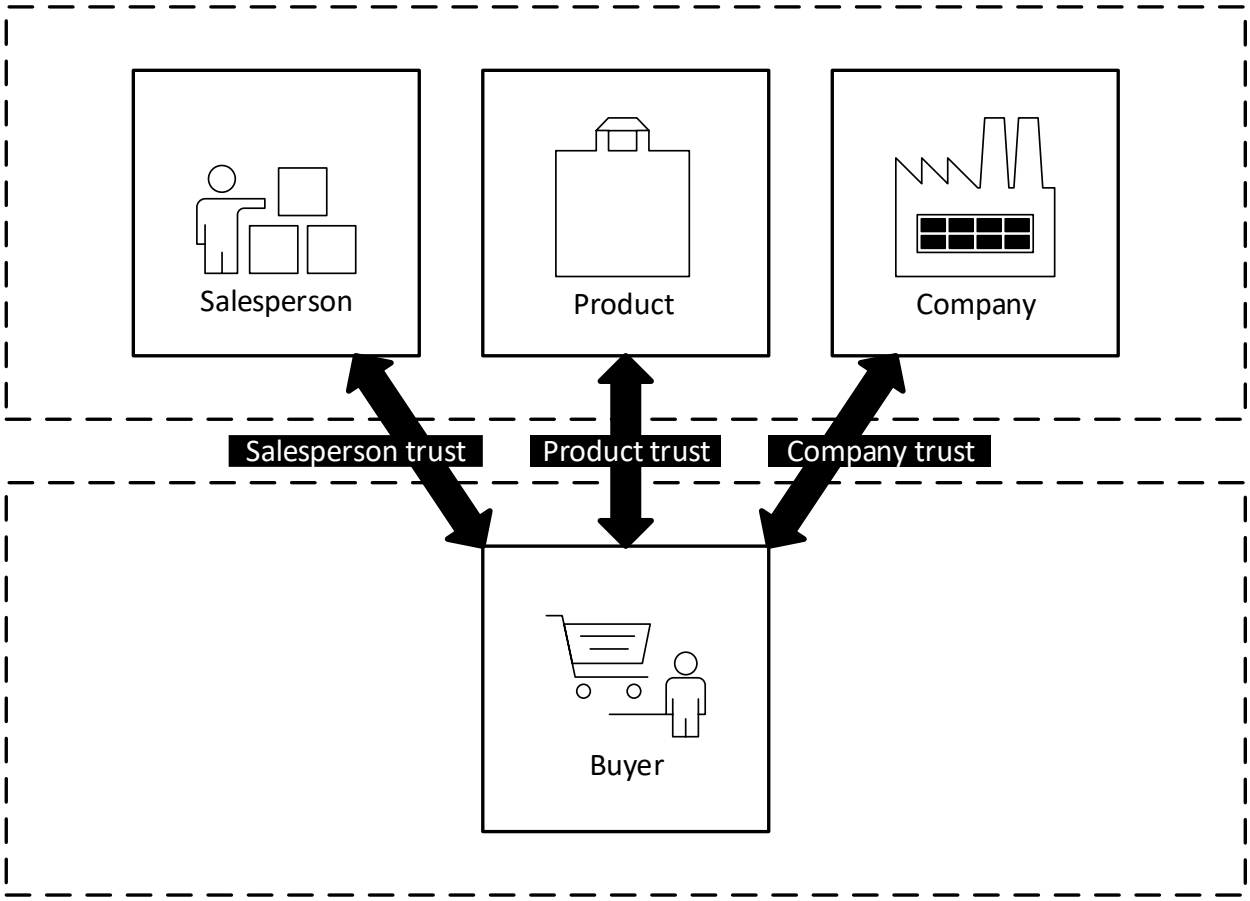


Figure 12: Components of trust according to Plank et al. (1999).

Plank et al. (1999) points out that, although these components of trust are most likely correlated, they are unique and need to be analysed separately.

Likewise, a few years earlier, Chow and Holden (1997, p. 277) also proposed to "introduce attitude toward the product (which also includes augmentations such as support and delivery)" along with the measure of salesperson trust and company trust in their model of buyer behaviour.

This research will therefore not only consider the trust of the buyer in the selling company and in the salesperson, but also in the offered products or services. Section 3.4.3 will review the literature on trust in the product/service in general and Section 3.5 will review the literature on trust in cloud computing as the main product/service discussed in this research.

3.4 Trust relationships

Having defined what is meant by company trust, salesperson trust and product trust, the following sections will review the existing literature on these three trust relationships.

3.4.1 Trust in the selling company

As explained in Section 3.3.1 and 3.3.2, inter-organisational trust is defined as the trust between the buyer and the selling company. The literature on inter-organisational trust has recognised trust as a critical success factor for buyer-seller relationships (Blomqvist, 2002; D. Ford, 1984; Friman, Gärling, Millett, Mattsson, & Johnston, 2002; Parkhe, 1998a; Sako, 1998) and as a fundamental bond in global collaboration (J. Child, 2001).

In buyer-seller relationships, trust increases predictability (Sako 1994), adaptability (Lorenz, 1988), cooperation (Razzaque & Boon, 2003) and strategic flexibility (Young-Ybarra & Wiersema, 1999), and it facilitates information sharing and open communication between companies (Blomqvist, 2002). At the same time trust reduces management costs (Williamson, 1993) and social complexity (Luhmann et al., 1979). Trust can also be a source of sustainable competitive advantage in buyer-seller relationships in general (Barney & Hansen, 1994; Shaw, 1997) and in internet services in particular (Warrington, Abgrab, & Caldwell, 2000).

However, despite the importance of trust for buyer-seller relationships, it “remains an undertheorized, under-researched, and therefore poorly understood phenomenon” (J. Child, 2001, p. 275). This view was also shared by other authors. In their review of the empirical research between 1990-2003 on inter-organizational trust, Seppänen et al. (2007, p. 250) argued that there “have not yet been any theoretically and empirically coherent attempts to measure trust in an inter-organizational context”. Their review revealed that the analysed studies varied in terms of the relationship type (e.g. buyer-seller, manufacturer-supplier or retail buyer-vendor relationships), the contextual background, the industry and the country. And although most studies conceptualised trust as a multidimensional construct, the number, role and content of these dimensions varied between them (Seppänen et al., 2007).

Table 16 provides an overview of the most influential literature on inter-organisational trust. The table summarises the subject of the publications as well as the methodology and findings of the studies. Papers that studied both, inter-organisational and interpersonal trust are discussed in the following section on trust in the salesperson (Section 3.4.2). Therefore, the number of studies listed in the section on salesperson trust is higher than the number of studies listed in Table 16. However, not all studies defined the object of trust and many studies referred to it in a passive way by using words such as party, actor and (exchange) partner (Seppänen et al., 2007). This means that it is not always clear if the authors are studying the trust in a company, the trust in a salesperson or the trust in a product or service. Seppänen et al. (2007) concluded that “measuring trust on the inter-organizational level is not very well developed and is potentially rather challenging”.

Table 16: Literature on inter-organisational company trust

Author(s)	Subject	Methodology	Findings
Ganesan (1994)	The role of dependence and trust for long-term buyer-seller relationships	Surveys with 124 U.S. retail buyers and 52 vendor representatives	Trust and dependence play key roles in determining the long-term orientation of both retail buyers and their vendors.
Aulakh et al. (1996)	The antecedents of trust and performance in cross-border marketing partnerships	Questionnaires with 257 managers of Fortune 500 firms	Bilateral relational norms and informal monitoring mechanisms are important in building interorganizational trust and improving market performance of international partnerships.
Nooteboom 1997	The effects of governance and trust on the risk perceived by agents of firms in alliances	Questionnaires with 10 suppliers of electrical/electronic components	Trust-related variables as well as others found to have significant effects on the perceived risk.
J. B. Smith and Barclay (1997)	The effects of organisational differences and trust on the effectiveness of selling partner relationships	Surveys with 105 sales representatives from two multinational computer industry companies	Trusting behaviours have a greater effect on perceived task performance than on mutual satisfaction. Dimensions of trustworthiness had both direct and indirect effects on satisfaction.
Sako and Helper (1998)	The determinants of inter-organizational trust in supplier relations	Surveys with 675 automotive component suppliers in the U.S. and 472 suppliers in Japan	Trust and opportunism were different for the U.S. and Japan. Long-term commitment, information exchange, technical assistance, and customer reputation facilitate trust.
Young-Ybarra and Wiersema (1999)	Determinants of strategic flexibility in a sample of	91 completed surveys from 132 alliances involving 251 companies	Trust was found to be positively related to flexibility while dependence was found to be negatively related to the

	strategic alliances involved in joint development agreements or joint research pacts		strategic flexibility of the alliance.
Dyer and Chu (2000)	An examination of the determinants of trust in supplier-automaker relationships in the U.S., Japan, and Korea.	Surveys with 135 U.S. suppliers, 101 Japanese suppliers and 217 Korean suppliers	Supplier trust is highly correlated with stable and consistent buyer processes/routines that represent credible commitments toward long term interactions-notably assistance-giving routines and supplier-selection routines that promote relationship continuity.
Handfield and Bechtel (2002)	The role of trust and relationship structure in improving supply chain responsiveness	Surveys with 97 purchasing managers in North American manufacturing firms	Supplier responsiveness can be improved by working to build trust within the relationship, even if buyers do not have much control over their suppliers.
Möllering (2002)	The impact of trustworthiness on the organisation of inter-firm relations	Surveys with 184 buyers of UK printing companies	The annexation of trust by transaction cost theory is rejected. Trust is a third force in transactions and can be more significant than market or hierarchy.
Norman (2002)	Factors associated with a firm's protection of knowledge from unwanted appropriation by an alliance partner	Surveys with 61 CEOs and key informants of computer, telecommunications, or microelectronics firms	Higher trust in a strategic alliance partner tends to reduce knowledge protection.
Coote et al. (2003)	Investigation into the antecedents of commitment in non-Western industrial marketing relationships	152 questionnaires from owners or CEOs of Chinese-owned businesses	Communication and conflict appear to be more important predictors of commitment than trust and similarity.
Kwon and Suh (2004)	Factors affecting the level of trust and commitment in supply chain relationships	Surveys with 171 supply chain managers (members of supply chain practicing organizations)	The trust of a company in its supply chain partner is highly associated with the asset investments (positively) and behavioural uncertainty (negatively) of both parties. Information sharing improves trust and reduces uncertainty.
T. Gao, Sirgy, and Bird (2005)	A conceptual model on whether the organizational buyer's decision-making uncertainty (DMU) can be reduced by the buyer's perceptions of supplier trust, supplier commitment, and	Questionnaires with 151 decision-makers of Austrian and Southern German automotive suppliers	Buyers' trust can be enhanced if buyers perceive suppliers to be trusting of the buyers and if buyers perceive the suppliers to be highly committed to the relationship. Buyers' perception of the supplier's dependence does not significantly increase buyers' trust, but it does have a direct effect on DMU.

	supplier dependence.		
Krishnan, Martin, and Noorderhaven (2006)	Examination of how uncertainty moderates the trust-performance relationship in alliances.	Questionnaires with managing directors and senior executives of 126 Indian firms with international alliances	The positive relationship between trust and performance is stronger under high behavioural uncertainty and weaker under high environmental uncertainty.
Hoffmann, Neumann, and Speckbacher (2010)	The effects of interorganizational trust on make-or-cooperate decisions	Questionnaires with 151 decision-makers of Austrian and Southern German automotive suppliers	Trust has an opportunism-mitigating effect that lowers the transaction costs of a collaborative exchange and an opportunism-independent effect that increases the transaction value of a collaborative exchange.
Kalkman and de Waard (2017)	Trust and control in inter-organizational disaster management projects	Documentation analysis and in-depth interviews with 9 military liaison officers involved in disaster management	Trust and control are complementary and mutually reinforcing.

It is also noteworthy that most of the research cited above was solely based on quantitative methods. As noted by Wright and Ehnert (2010, p. 119), “the dominant discourse among trust researchers is positivistic”. This is all the more incomprehensible since there is no all-encompassing and agreed method to measure inter-organisational trust (Seppänen et al., 2007). The question arises how trust can be quantified if different conceptualisations are applied to the same theory and how quantitative results can be compared, replicated and validated if there is no common denominator between the studies. The generalisability of much published research on this issue is therefore problematic. For example, Möllering (2002, p. 158) concluded that “the role of trust is not easily quantifiable and therefore this area of research can be expected to benefit greatly from qualitative studies”. And since “the concept of trust is apparently not easily quantifiable, it seems obvious that qualitative empirical studies and piloting are also called for before quantitative surveys are carried out” (Seppänen et al., 2007, p. 261).

Consequently, as outlined in Chapter 4, the current research will apply qualitative methods to study the origins and reasons for trust or distrust between the parties involved. The qualitative research method is particularly suited to interpret social processes and to get a deep understanding of human behaviour and individual

meaning in a real-world context such as the importance of the different trust relationships that exist between German companies and U.S. cloud providers.

This section has analysed the literature on inter-organisational trust and has argued that there have not yet been any coherent attempts to study inter-organizational trust and that it was not always clear if the studies focused on the trust between the buyer and the selling company or on other relationship types. Additionally, most of these studies followed a quantitative research method which calls for more qualitative work in this field.

The following section will specifically address the literature on trust in the salesperson and the impact of the salesperson on trust in buyer-seller relationships.

3.4.2 Trust in the salesperson

There is a large volume of published studies describing the role of trust between the buyer and the salesperson. Most of these studies have revealed that it is not just the trust of the buyer in the selling company that acts on the buyer-seller relationship but also the trust of the buyer in the salesperson. In many business transactions, the salesperson is the primary or even the only contact point for the buyer, both before and after the purchase (Crosby, Evans, & Cowles, 1990).

Trustworthiness is ranked as one of the most important characteristics a seller can have (Hayes and Hartley 1989) and salesperson trust can be seen as a necessary antecedent to trust in the selling company (Chow & Holden, 1997). Trust in a salesperson can even be more strongly related to buyer commitment than trust in the selling company (Ganesan & Hess, 1997). Table 17 compares the literature of trust in the salesperson in terms of their context, the methodology applied to the studies and their findings. Since not all studies can be discussed in detail in this section, Table 17 provides an overview of some of the literature on salesperson trust from the 1970s until today.

Swan, Bowers, and Richardson (1999) conducted a first comprehensive review of the literature on salesperson trust. Drawing on an extensive range of sources, the authors analysed the literature for the measurements, determinants and consequences of trust. A key result of their literature review was that trust had a positive impact on the behaviour of the buyer such as buying the offered products or services. If the buyer

trusted the salesperson, the probability of a purchase above the median increased from 39% to 64%. Trust in the salesperson also had other positive consequences. The probability of customer satisfaction being higher than the median increased from 24% to 76% and the probability of positive attitudes towards the salesperson being above the median raised from 36% to 64%. Swan et al. (1999, p. 106) concluded that the development of trust between the salesperson and the buyer was “a worthy managerial objective”.

Table 17: Literature on salesperson trust

Author(s)	Subject	Methodology	Findings
Busch and Wilson (1976)	Analysis of the impact of differential levels of a salesman's expert and referent social power bases on the customer’s trust in the salesperson.	Experiment with 187 male junior level students	Expertise is generally more effective than referent power in producing the desired customer changes.
Schurr and Ozanne (1985)	Study to clarify the effects of trust and tough/soft bargaining postures on buying behaviour.	Bargaining experiment with 103 MBA students	A seller's expected trustworthiness plus toughness in bargaining led to higher levels of buyer-seller cooperation and agreement and a higher level of buyer concessions.
Swan, Trawick, and Silva (1985)	Study on how industrial salespeople gain the trust of their customers.	Questionnaire with 42 medical salespeople	Trust increases as the customer thinks that the salesperson is dependable, honest, competent, customer oriented, and likeable.
Swan, Trawick, Rink, and Roberts (1988)	Trust was conceptualized as the extent to which a salesperson exhibited five attributes: dependable, reliable, honest, responsible, and likeable.	187 completed questionnaires from purchasing agents and managers	Results indicate that overall trust is significantly related to the assumed trust components “dependable, reliable, honest, responsible, and likeable”, with the most key factor to the buyer being dependability.
Jon M. Hawes, Mast, and Swan (1989)	An examination of the perceptions of sales representatives and purchasing executives in relation to the process of earning the buyer's trust.	Survey with 193 sales representatives and 173 purchasing executives	The sales representatives overestimated the trust earning potential of the “likeable,” “competent,” and “dependable” constructs and held an inflated view of the overall extent to which they were trusted by purchasing executives.
Crosby et al. (1990)	A relationship quality model is advanced and tested that examines the nature, consequences, and antecedents of the quality of the salesperson-customer relationship.	Questionnaires from 296 consumers with life insurances	Sales opportunities depend mostly on relationship quality (i.e., trust and satisfaction). Relational selling behaviours such as cooperative intentions, mutual disclosure, and intensive follow-up

			contact produce a strong buyer-seller bond.
A. Sharma (1990)	The first experiment investigated the effect of salesperson credibility on buyers' product evaluations and buying intention. The second experiment investigated the interaction of initial product expectations and salesperson credibility on product evaluations, buying intentions and cognitive responses.	First experiment with 45 students, second experiment with 65 students	Salesperson credibility has a positive effect on product evaluation and buying intention when buyers have no prior knowledge of a brand or when buyers have low expectations of a brand. Salesperson credibility did not have an effect when customers had high expectation of a brand.
Lagace, Dahlstrom, and Gassenheimer (1991)	The impact of ethical salesperson behaviour on relationship quality.	Questionnaire completed by 90 medical doctors	Ethical behaviour and expertise of the salespersons impact both trust of the salesperson and satisfaction with the exchange.
Jon M. Hawes, Rao, and Baker (1993)	Importance which consumers place on various salesperson attributes in the retail purchase of durable goods.	In-home personal interviews with 506 consumer households	From an original list of 25 salesperson characteristics, exploratory factor analysis was used to identify seven underlying dimensions, and trustworthiness was found to be of greatest importance.
Jon M Hawes, Strong, and Winick (1996)	The impact of five different closing techniques and a no-close condition on the prospect's trust toward the salesperson was assessed.	After-only field experiment that included 238 industrial purchasing executives	The highest-ranking mean score for prospect trust occurred in the “no-close” scenario. This provides some evidence that using a closing technique may diminish prospect trust.
Strutton, Pelton, and Tanner Jr (1996)	Investigation of the possible influence that the use of these ingratiatory behaviours has on the level of trust buyers place in salespeople.	Questionnaires answered by 251 salespeople	Offensive ingratiatory behaviours are generally associated with lower levels of buyer trust in salespeople, whereas certain defensive ingratiatory behaviours were shown to positively influence buyer-seller trust.
Chow and Holden (1997)	Trust in the salesperson and trust in the company supplying the products, are hypothesized to influence loyal buying behaviour.	Questionnaire sent to buyers of electronic circuit boards with 155 respondents	Trust is a multifaceted phenomenon, manifested in trust in the salesperson and trust in the company. Buyer's attitude toward the product is not a significant antecedent to buyer loyalty.
Doney and Cannon (1997)	Impact of supplier firm and salesperson trust on a buying firm's current supplier choice and future purchase intentions.	Three-wave mail survey with 210 buying/ purchasing executives	Trust of the supplier firm and trust of the salesperson influence a buyer's anticipated future interaction with the supplier. The process of building customer trust creates strong buyer-seller bonds and enhances loyalty.

A. Zaheer et al. (1998)	Investigating the role of trust in interfirm exchange at two levels of analysis and assess its effects on negotiation costs, conflict, and ultimately performance.	Questionnaires with 107 buyer-supplier interfirm relationships in the electrical equipment manufacturing industry using a structural equation model	Interpersonal and interorganizational trust are related but distinct constructs, and play distinct roles in affecting negotiation processes and exchange performance.
Jule B. Gassenheimer and Manolis (2001)	The effects of salesperson and organizational trust between buyer dependence and future purchase intentions.	Questionnaires with 138 members of the National Association of Purchasing Management (NAPM)	Although salesperson trust mediates relationships between both product customization and future intentions and number of suppliers and future intentions, organizational trust does not.
Kennedy, Ferrell, and LeClair (2001)	A positive model of consumers' trust of salesperson and manufacturer is developed which provides suggestions for improving relationships and increasing buyer-seller trust.	Questionnaires from 786 car buyers.	The findings indicate that buyer-seller trust results from salesperson competence, low pressure selling tactics, service quality, manufacturer ethical concern, and a general tendency to trust others.
A. Wong and Sohal (2002)	Examination of the concept of trust and relationship quality on salesperson level and store level.	Questionnaires with 1,261 retail customers	The findings of this research revealed the role of trust and commitment and their impact on relationship quality.
Young and Albaum (2003)	A two-country study is conducted looking at the perceptions of buyers regarding the trust they place in direct selling salespeople.	Questionnaires from Australia (120) and the U.S (166)	Three distinct measures of trust and two related measures, based on scales developed for use in contexts other than direct selling, are utilized.
Belonax, Newell, and Plank (2007)	The study investigates whether buyer perceptions of trust and expertise of the salesperson and the company they represent vary by the perceived importance of the purchase decision.	Mail surveys with 269 members of the Institute for Supply Management (ISM)	The results indicate that buyer perceptions of supplier and salesperson expertise and trust were higher in minimally important purchases than in extremely important purchases.
Rutherford (2007)	This study is one of the first studies to fully address the relationship that business-to-business buyers have with both the selling firm and salesperson within an integrated model.	Online survey with 199 participants	The selling firm controls the relationship and the buyer views that relationship primarily being with the selling firm, but if the selling firm allows a boundary spanner to harm the relationship the buyer may terminate the relationship.
Fang, Palmatier,	The effects of trust at three distinct	Dyadic	Results indicate that trust at each

Scheer, and Li (2008)	organizational levels in a marketing collaboration.	survey and longitudinal objective performance data from 114 international joint ventures in China	level has unique effects but similarly influences the collaborating firms' resource investments or the collaborative entity's use of those resources.
Wood, Boles, Johnston, and Bellenger (2008)	To assess the nomological validity of trust-related measures, this research uses an item-level measurement meta-analysis based on correlations from studies that measure trust-related constructs in the context of a buyer's assessments of sellers.	Meta-analysis based on correlations from 32 studies	Analysis reveals that 16-item measures converge into three constructs that are indicative of the seller's credibility, expertise, and compatibility and three items each that are indicative of trust and trustworthiness.
Guenzi and Georges (2010)	Explore drivers and consequences of customer trust in the salesperson in the financial services industry.	Partial least squares (PLS) on a sample of 150 customers in the Italian banking industry	Trust in the salesperson positively influences a customer's intentions to re-buy/cross-buy and to recommend, while it decreases a customer's intention to switch to competitors.
Newell, Belonax, McCardle, and Plank (2011)	Investigate the connection between sales behaviours and buyer assessment of salesperson attributes and loyalty.	Questionnaires with 433 members of the Institute for Supply Management (ISM)	Consultative task and personal relationship behaviours play a vital role in influencing buyer perceptions of expertise, trust, and relationship loyalty.
M. Srinivasan and Srivastava (2012)	The impact of the antecedents of trust including the buyer's perception of equity with the salesperson and salesperson's benevolence on development of trust in a buyer-salesperson relationship is examined.	Survey with 218 members of the Institute of Supply Management (ISM)	Positive relationship between salesperson benevolence and buyer's perceived equity with the salesperson and trust in the salesperson.
Twing-Kwong, Albaum, and Fullgrabe (2013)	Trust in the customer-salesperson relationship in three major retail types within China.	Street intercept personal interview surveys with 554 Chinese consumers	Increased satisfaction by consumers with the salesperson leads to a higher level of both cognitive and affective trust. Intention to maintain a relationship with the salesperson is positively related to both types of trust.
D.-J. Yang and Wu (2014)	Importance of the competence in a salesperson's performance and the mechanism underlying the relationship between competence and performance.	Survey with 165 salespersons working in a life insurance company and 338 customers	The mediation of the effect of social and professional competence on objective salesperson performance differed depending on affective trust and cognitive trust.

Bateman and Valentine (2015)	This study assessed whether a salesperson's relational customer orientation could trigger improved evaluations of a salesperson's ethical treatment of a customer, increased trust in the salesperson, and stronger intentions to purchase.	Convenience sample of 280 adult consumers (non-students) with varying amounts of sales and management experience	The results indicated that a relational selling approach resulted in increases in the three indicators of sales effectiveness.
Gustafsson and Folmerz (2015)	This study develops an understanding of how to create trust in business-to-business relationships. In order to develop this understanding, an examination on what factors that are affecting trust and also how sellers behave is investigated.	Face-to-face semi-structured interviews with 12 Swedish salespeople	Trust and honesty are important for sellers when establishing long-term relationships. The study shows that aspects affecting trust in this context is expertise and cooperation whereas communication and social behaviour affect cooperation.
Ashnai, Henneberg, Naudé, and Francescucci (2016)	A nomological model was built around an overall framework consisting of three main groups of business relationship characteristics: attitudes, behaviours, and outcomes.	331 middle or senior managers in the UK who were knowledgeable about supplier relationships	Inter-personal trust and inter-organizational trust were found to be two distinct constructs, with the results of a structural equation analysis supporting the overall model that was developed.
Guenzi, De Luca, and Spiro (2016)	Examine the impact of customer perceptions about a salesperson's combined use of adaptive selling (AS) and selling orientation (SO) on customer trust in the salesperson.	Surveys with 134 business-to-business (B2B) buyers	When purchase importance for the customer is low, salespeople should combine AS and customer orientation. When purchase importance is high, salespeople can only generate more trust by increasing customer orientation/reducing SO.
Jaramillo and Valenzuela (2016)	Impact of the salesperson's empathy on customer loyalty, satisfaction and trust.	Surveys with 300 customers from two Chilean banks	Both customer orientation and salesperson's empathy play a critical role in influencing customer's opinions about their relationship with a firm and eventually lead to supplier loyalty.
Newell, Wu, Leingpibul, and Jiang (2016)	The importance of corporate and salesperson expertise and trust in building business-to-business relationships in China.	Surveys with 181 Chinese business professionals with purchasing responsibilities taking MBA classes	Trust and expertise play key roles in developing long-term business-to-business associations in China.
Friend, Johnson, and Sohi (2018)	The role of customers' existing propensity to trust salespeople in	Surveys with 131 newly acquired customer key	The higher a customer's propensity to trust, the

	determining their trust of salespeople in newly formed business-to-business relationships.	informants and 47 B2B salespeople	greater his/her trust in the salesperson.

More recent studies on the trust relationship between buyers and the salesperson confirmed these results. Kennedy et al. (2001) suggested that a competent salesperson creates satisfaction which leads to trust of the buyer in the salesperson as well as the selling company. A. Wong and Sohal (2002) found that salesperson trust is positively related to company trust and that the trust of a buyer in the selling company can drop if the existing buyer-salesperson relationship is disrupted by a job change or other events.

According to other studies, trust in the salesperson is positively related to customer purchase intentions (Bateman & Valentine, 2015) and it does not only increase the probability of a customer to re-buy products and services, it also decreases the likelihood that a customer is switching to a competitor (Guenzi & Georges, 2010). On the other hand, the salesperson can have a direct negative impact on the trust relationship between the buyer and the selling company (Rutherford, 2007).

The benevolence of a salesperson (M. Srinivasan & Srivastava, 2012) but also the personal relationship behaviour and the consultative task behaviour of a salesperson (Newell et al., 2011) significantly affect the buyer's perceived trust in the salesperson. This is even more true in a situation where the buyer is facing some degree of risk or uncertainty (M. Srinivasan & Srivastava, 2012). Hence, several studies recommended that companies should invest in hiring sales people with the right skills (Bateman & Valentine, 2015; Kennedy et al., 2001; Newell et al., 2011) to meet customer needs and solve their problems. Additionally, companies should design training concepts (Bateman & Valentine, 2015; Kennedy et al., 2001; Newell et al., 2011; Newell et al., 2016) to help their sales people building trust with their customers and become more competent and professional.

However, not all authors agreed that the salesperson had a direct positive impact on trust in buyer-seller relationships. Rutherford (2007, p. 108) suggested that the selling company "controls the relationship and the buyer views that relationship primarily being with the selling firm" and not with the salesperson. He concluded that the

salesperson only has an indirect positive impact on the continuance of this relationship.

As discussed in the previous section, the trust in the selling company was mainly based on quantitative methods. Table 17 shows that the findings of the studies on trust in the salesperson also relied heavily on quantitative research. As already written above, this calls for qualitative work in this subject area. The current research will address this gap by following a qualitative method through semi-structured key informant interviews.

Another criticism of much of the literature on trust in the salesperson is that most of the studies were conducted in the U.S. or published in U.S. journals such as the Journal of Marketing Research by the American Marketing Association. This may also explain the preference for quantitative studies since “editorial decisions about what is accepted for publications, especially in flagship journals”, have a strong impact on the choice of the research method (Silverman & Marvasti, 2008, p. 484). It can therefore be concluded that there is a need for qualitative research as a counterweight to the substantial number of quantitative studies.

The following section will review the literature on trust in the product or services.

3.4.3 Trust in the product

There is much less literature on the subject of “product trust” than on salesperson trust or on inter-organisational trust relationships. Table 18 provides an overview of the studies on product trust and compares the methodologies and findings of the publications.

Table 18: Literature on product trust

Author(s)	Subject	Methodology	Findings
Chow and Holden (1997)	The three theoretical constructs - trust in company, trust in salesperson, and attitude toward the product - are assumed to influence purchasing behaviour indirectly through the purchasing strategies of the buyer	Questionnaires with 155 buyers of electronic circuit boards	Trust is a multifaceted phenomenon, manifested in trust in the salesperson and trust in the company. Buyer's attitude toward the product is not a significant antecedent to buyer loyalty.
Plank et al. (1999)	Trust is conceptualized specifically within a business-to-business	Single-wave questionnaire mailing with 568	A ten-item, three factor scale was developed incorporating multiple objects of trust

	sales context as containing three correlated components: salesperson trust, company trust, and product/service trust.	purchasing managers	(salesperson, company and product/service). The scale factored as expected, demonstrated internal consistency, and was significantly related to sales effectiveness.
Kennedy et al. (2001)	A model of consumers' trust of salesperson and manufacturer is developed which provides suggestions for improving relationships and increasing buyer-seller trust.	82 questionnaires with car buyers in the U.S.	Product quality was found to be the strongest indicator of ownership satisfaction, not service quality, ethical concern of the manufacturer or salesperson characteristics.
Brickau, Huth, Tysiak, and Chaston (2003)	The impact of trust in a finance setting, the importance of trust towards three dimensions, which antecedent client-trust build towards these dimensions	Questionnaires with 321 respondents from the financial sector	Trust in the consultant/advisor is more important than trust in the product/service/solution offered. Trust in the company is not more important than trust in the product/service/solution offered.

In an empirical investigation of trust in buyer-seller relationships in a service environment, Brickau et al. (2003) found that all three trust relationships were of similarly great importance. In the specific context of their research, salesperson trust was the most important dimension, followed by product trust and company trust. However, according to the authors, the salesperson trust was especially important in the first contacts with the buyer but over time the salesperson trust became less relevant and the trust in the product and in the selling company became more important (Brickau et al., 2003). Huth (2004, p. 308) summarised that “interpersonal trust seems to be of higher importance compared to product trust” and “product trust seems to be of greater importance than organisational trust” for both buyers and sellers.

In contrast, Kennedy et al. (2001, p. 81) found that product quality was “the strongest indicator of ownership satisfaction”, not the qualities of the salesperson or the selling company. Another finding was that product quality did not help to create salesperson trust. The authors concluded that salesperson trust was dependent on factors outside the product itself and that buyers differentiated between the roles of the selling company as the producer of the products and the salesperson who matches products with the needs of the buyer (Kennedy et al., 2001).

A question that needs to be asked, however, is why the number of literatures on trust in the product/service is quite limited. One reason could be that the focus is more often on the quality and functionality of a product and not explicitly on trust. As described in Section 3.3.2, product trust can be defined as “the belief that the product/service will fulfil its functions as understood by the buyer” (Plank et al., 1999, p. 62). These functions can include parameters such as reliability, performance, security, efficiency, sustainability and durability. It depends therefore on the product/service itself how to measure each of these functions and if they meet the expectations of the buyer.

In case of the current research, the product/service is the public cloud computing service offered by an U.S. cloud provider. The following section will therefore review the literature on trust in cloud computing services.

3.5 Trust in cloud computing

Cloud computing is a special form of online business. With cloud computing, the seller is not only selling something over the Internet to the buyer (like in an online shop) but is selling the Internet service itself. Cloud computing is advertised over the Internet, can be ordered over the Internet, purchased, configured and consumed over the Internet. And the service itself is a part of the Internet.

As outlined in Chapter 2, cloud computing is “a question of trust” (Everett, 2009, p. 6) and trust is a “major issue with cloud computing irrespective of the cloud model being deployed” (Onwubiko, 2010, p. 282). A number of researchers have stressed the importance of trust in the adoption of cloud computing services. According to the authors, the increasing demand for cloud services unfolds an “increasing need for trust management in cloud computing” (Selvaraj & Sundararajan, 2017, p. 329) and plays an important role in the relationship between cloud provider and cloud consumer (Chiregi & Navimipour, 2016; Y.-C. Liu, Ma, Zhang, Li, & Chen, 2011). They argued that “the trustworthiness of cloud services is a critical issue” (Tang, Dai, Liu, & Chen, 2017, p. 302) and that “trust is one of the most challenging issues in the emerging cloud computing era” (Sidhu & Singh, 2017, p. 81). Similarly, S.M. Habib, Ries, and Muhlhauser (2010, p. 415) wrote that “the establishment of trust in the cloud environment is a major issue for the success of cloud computing”, Manuel (2015, p. 281) claimed that trust is “one of the biggest challenges of cloud technology” and Pathan and Mohammed (2015, p. 77) even described building customer trust as a

“huge problem in the cloud computing paradigm”. Khaled M Khan and Malluhi (2013, p. 94) even claimed that “trust is more important than money and will ultimately determine cloud computing’s success”.

Trust was also found to be “a strong predictor of deployment success and key factor in effective collaboration and assurance that the client organization’s cloud strategy is implemented in its best interests” (Garrison, Kim, & Wakefield, 2012, p. 67). As maintained by Chahal and Singh (2017, p. 338), people “still have a lot of apprehensions resulting from the lack of trust on cloud service providers”. And the lack of trust has been identified as “one of the key barriers to the adoption of cloud computing services” (Lynn, Van Der Werff, Hunt, & Healy, 2016, p. 191). Likewise Emeakaroha et al. (2017, p. 689) stated that “trust issues have been identified as a factor holding back cloud adoption” and Beugelsdijk, Koen, and Noorderhaven (2009) stated that trust issues hinder the speedy adoption of cloud computing services. This view was also shared by Ko et al. (2011, p. 38) who argued that “the key barrier to widespread uptake of cloud computing is the lack of trust in clouds by potential customers”.

Cloud computing services are expected to be able to support critical business applications (e.g. smart grid systems) and cloud customers should be provided with evidence of the trustworthiness of the cloud computing service without having to know the infrastructure details (Abbadi & Alawneh, 2012, p. 1073). As pointed out by S.M. Habib et al. (2012), trust becomes particularly important when data processing is taking place across geographically spread data centres and resources are distributed beyond a definable perimeter, which is a common scenario in cloud computing services. However, as maintained by Chiregi and Navimipour (2016, p. 280), trust is “not written into an agreement” but is “something earned”.

Already before the Internet connected all aspects of everyday life, the concept of trust was studied by computer scientists (Jøsang, 1996). And as Internet technologies became more established, attention was turning to trust as a key factor for the success in the online environment such as e-Commerce, e-Business, online shops and online banking (Beldad et al., 2010; Corritore, Kracher, & Wiedenbeck, 2003; Dinev et al., 2006; Gefen & Straub, 2003; Sirkka L. Jarvenpaa, Tractinsky, & Saarinen, 1999; M. K. Lee & Turban, 2001; Lifen Zhao, Koenig-Lewis, Hanmer-Lloyd, & Ward, 2010; D.

Harrison McKnight et al., 2002; Shankar, Urban, & Sultan, 2002; Yao-Hua Tan, 2000). However, “while successful models of e-commerce use showing the importance of privacy concerns and trust beliefs have been developed, all of them were U.S. centred and used only the U.S. as the cultural base” (Dinev et al., 2006, p. 397).

Uusitalo et al. (2010, p. 719) claimed that “the importance of trust attains a new level in cloud services” and that trust assessments in cloud computing environments are more complicated than in the real world since there are no physical or facial cues to use and appropriate government agencies or certification authorities are still missing or might not be applicable. In a public cloud environment, the control of data is moved away from the cloud consumer which requires the cloud consumer to trust the cloud provider (Uusitalo et al., 2010). The “fluid nature” of cloud computing makes it a “moving target when even trying to determine what questions we should be asking regarding trust” (Michael, 2009, p. 3).

Several authors reviewed the literature on cloud computing from different perspectives. Martens and Teuteberg (2012) applied quantitative content analysis to give an overview of cloud computing studies and included data comprises research and practitioner-oriented articles. However, the authors only mentioned trust in the cloud provider once and did not discuss the impact. The focus of the review of Hoberg, Wollersheim, and Krcmar (2012) was cloud computing research from a business perspective and the authors structured the studies according to cloud computing characteristics, determinants for adoption, business impact and governance mechanisms. Though, Hoberg et al. (2012) did not identify trust as a factor and did not discuss the influence of trust in the business perspective on cloud computing. In their review of literature on cloud security concerns, Khorshed, Ali, and Wasimi (2012) proposed solutions to mitigate these threats. Although the authors identified “trust issues, security threats, security risk and some other specific cloud computing related issues” as “the main gaps of cloud computing”, the role and influence of trust was not discussed in more detail (Khorshed et al., 2012, p. 835).

Venters and Whitley (2012) proposed a classification scheme to structure cloud computing research publications which is based on interviews with cloud providers and cloud customers. The authors aimed to create a framework which is structured around the most importance cloud computing characteristics from the point of view of

cloud customers and applied the framework to existing literature. A conclusion of their research was that “like other outsourcing arrangements cloud computing demands trust, and to gain trust, knowledge of counter-parties is required” (Venters & Whitley, 2012, p. 193). However, the authors did not discuss this topic any further but referred to future research. Likewise, H. Yang and Tate (2012) offered a framework to classify existing and future cloud computing research publications. The authors structured existing research articles according to this scheme which is categorized in business issues, technology issues, conceptualizing cloud computing and domains and applications. H. Yang and Tate (2012, p. 43) identified trust as a “business issue” along cost, pricing, legal issues, ethical issues, privacy and adoption and found four business issues articles mentioning trust. Nevertheless, there was no further discussion of the importance of trust for cloud adoption.

The focus of the literature review by Ermakova, Huenges, Erek, and Zarnekow (2013) was on cloud computing research in the healthcare and aimed to identify the state of research and determine the potential areas of future research in the domain. Trust or trustworthiness were mentioned in the article but not discussed as a factor for cloud adoption. In a more recent review, S. Schneider and Sunyaev (2016) summarized the academic literature on IT outsourcing and cloud computing by identifying factors for IT sourcing decisions and compared the findings. The review did not discuss the role of trust in these decisions. In their review on cloud computing literature, H. Yang and Tate (2009) and Hoberg et al. (2012) concluded that the bulk of the literature was coming from the computer science discipline and tried to solve trust issues with technological measures. Overall, there seems to be some evidence to indicate that many researchers “focus exclusively on the technical aspects of cloud computing” (Leimeister, Böhm, Riedl, & Krcmar, 2010, p. 1) and “only few or no studies are focusing on the behavioural characteristics of cloud computing adoption […] exist” (Obeidat & Turgay, 2013, p. 161).

Nevertheless, in the last years, there has been an increasing amount of literature on trust in cloud computing. However, several publications that carried the word “trust” in the title merely touched the relationship between cloud computing and trust but rather focused on topics such as cloud computing and policy (e.g. Jaeger et al. (2008)), cloud computing and privacy (e.g. Bhosle and Kasurkar (2013)), cloud computing and

certifications (e.g. J. Huang and Nicol (2013)) and cloud computing and security issues (e.g. Roberts II and Al-Hamdani (2011); P. Sharma, Sood, and Kaur (2011)). Moreover, these publications did not provide any empirical data and simply proposed further research topics while not providing much additional insight. A large number of studies focused on technical and/or security issues with cloud computing (e.g. K.M. Khan and Malluhi (2010), Zhang, Cheng, and Boutaba (2010), Kanwal, Masood, Ghazia, Shibli, and Abbasi (2013), Jaiganesh, Aarthi, and Kumar (2015), Jabbar, Naseer, Gohar, Rho, and Chang (2016)) or on the threats and opportunities of cloud computing for certain sectors such as the telecommunication industry (e.g. Martucci et al. (2012)).

As described in Section 2.1, cloud computing is a relatively recent technology. Therefore, the number of studies about cloud computing and trust is limited. Table 19 gives an overview of the recent literature on trust in cloud computing services and compares the methodologies and findings of the studies.

Table 19: Literature on trust in cloud computing

Author(s)	Subject	Methodology	Findings
Jaeger et al. (2008)	This article explores the nature and potential of cloud computing, the policy issues raised, and research questions related to cloud computing and policy.	No empirical research	Cloud computing will likely serve to further highlight the ever-widening gaps between the capacity of technology and the focus of policy.
K.M. Khan and Malluhi (2010)	How cloud providers can earn their customers' trust when a third party is processing sensitive data in various countries.	No empirical research	To gain consumers' trust, cloud providers must offer better transparency and more consumer control of data and processes.
Uusitalo et al. (2010)	Interview study on trust and cloud services, covering the nature, measurement and experiencing of trust.	Semi structured theme interviews with 33 subject matter experts from Finnish companies, government organisations and research organisations	The key factor affecting perceived trust in cloud services is Brand, including such sub-aspects as reputation, image, history and name of the CSP. Security & Privacy and Transparency and Reliability were the second and third most important aspects.
Roberts II and Al-Hamdani (2011)	This paper describes numerous security issues facing cloud computing and cloud operating systems.	No empirical research	A method for allowing the user to select specific security levels of security for items and make a list of security items that all users should be

			aware of before opting to use cloud-based services.
Chakraborty and Roy (2012)	SLAs vary in description, length, and types of information released. Therefore, cloud consumers need a better way of estimating 'trustworthiness' of a cloud provider.	Untested theoretical framework	Framework for estimating trustworthiness of a cloud using a quantitative model of trust based on parameters that can be extracted from SLA.
Garrison et al. (2012)	Success factors for deploying cloud computing.	Survey with 314 IT managers in manufacturing, financial, logistics, IT, and education sector.	Cloud-vendor relationships characterized by trust are critical for cloud deployment and the promise of gaining advantage in a competitive market.
S.M. Habib et al. (2012)	Comparison of existing trust and reputation (TR) models for cloud computing.	Survey and analysis of TR systems/models	Requirements for trust and reputation models (or systems) to support the consumers in establishing trust on Cloud providers.
Martucci et al. (2012)	List of challenges and privacy, security and trust requirements that must be considered before cloud computing can be deployed by telecommunication providers.	No empirical research	Set of privacy, security and trust requirements that must be considered before cloud computing solutions can be fully integrated and deployed by telecommunication providers.
Muchahari and Sinha (2012)	There are several concerns relating to security, privacy and trust that hinders the adoption of cloud despite several beneficial features.	Untested theoretical framework	Development of a trust management architecture which consist of a "Cloud Service Registry and Discovery" component, a "Trust Calculator" and a "Dynamic Trust Monitor".
Bhosle and Kasurkar (2013)	Trust and privacy concern of cloud customers.	No empirical research	Customers should be confident about the services and interactions they have with their providers in terms of security, integrity and trust.
Noor, Sheng, Zeadally, and Yu (2013)	Overview of cloud service models and survey of the main techniques and research prototypes that efficiently support trust management of services in cloud environments.	Literature review of 30 trust management prototypes	Presentation of a generic analytical framework that assesses existing trust management research prototypes in cloud computing and relevant areas using a set of assessment criteria.
Kanwal et al. (2013)	An assessment of criterion for the evaluation of trust models containing the	No empirical research	Proposed assessment criteria for evaluation and analysis of trust models in cloud computing.

	essential features that are mandatory for trust establishment in Cloud environment.		
Fan and Perros (2014)	Trust management in multi-cloud environments based on a set of distributed Trust Service Providers (TSPs).	Simulation experiment, no empirical data	TSP-based trust management architecture, which is designed to perform the tasks of trust information eliciting, processing, and evaluation of CSPs in a multi-cloud environment.
Manuel (2015)	Trust model based on past credentials and present capabilities of a cloud resource provider.	Simulation experiment, no empirical data	A trust management system is proposed, and it is described how a service level agreement is prepared combining quality of service requirements of user and capabilities of cloud resource provider.
Chiregi and Navimipour (2016)	This paper evaluates the trust by considering the influence of opinion leaders on other entities and removing the troll entities' effect in the cloud environment.	Simulation experiment, no empirical data	A method for opinion leaders and troll entity identification using three topological metrics, including input-degree, output-degree and reputation measures.
El-Gazzar et al. (2016)	The most critical issues enterprises are confronted with when making cloud computing adoption decisions.	Delphi panel with 34 experts from different domain backgrounds plus 16 follow-up interviews	The findings indicate that security, strategy and legal and ethical issues are the most important.
Lansing and Sunyaev (2016)	Development of a conceptual model that describes trust in cloud services.	Review of 43 studies on trust in IT outsourcing and trust in IT artefacts	A conceptual model that provides a typology of constructs for trust in cloud services, defines trust-building antecedents, and develops 19 propositions describing the relationships between trust constructs and between trust constructs and trust-building antecedents.
Macías and Guitart (2016)	This article addresses the problems with online reputation systems for cloud computing by describing a decentralised (peer-to-peer) trust model that does not require the intervention of a central entity to manage it.	Simulation experiment, no empirical data	A model that includes mechanisms to allow participants to avoid dishonest behaviour from other peers where each client statistically analyses the external reports about providers and updates the trustworthiness of the peers.
Noor, Sheng, Maamar, and Zeadally (2016)	A proposed (updated) framework for analysing trust management Systems.	Literature review of 30 trust management systems	Presentation of a generic analytical framework that assesses existing trust management research prototypes in cloud computing and relevant areas

			using a set of assessment criteria.
Varalakshmi and Judgi (2016)	This paper aims to select the Trustworthy Service Provider (TSP) by evaluating trust based on in-context feedback from customers, global advisory and third parties.	Simulation experiment, no empirical data	Creation of a multifaceted trust management framework to increase the job-success rate, to improve the worthiness of the payment made by the provider to the customers and to enhance the quality of service.
Chiregi and Navimipour (2017)	Trust evaluating mechanisms in cloud computing.	Literature review	Integrity, security, availability, reliability, dependability, safety, dynamicity, confidentiality and scalability were defined as characteristics.

According to an interview study conducted by Uusitalo et al. (2010), the most important factor influencing perceived trust in cloud computing services was not a functional trust influencer such as security but the non-functional aspect of the cloud provider's brand including reputation, image, history and name of the cloud provider. The study also revealed that positive experiences with the cloud service only retained the level of trust in the cloud provider but negative experiences were "quick to deteriorate trust" (Uusitalo et al., 2010, p. 719). The authors concluded that it was therefore vital for cloud providers to actively build a trust relationship with cloud consumers. In case of the current study, the non-functional aspects will be studied by analysing the importance of the trust relationship between the buyer and the selling company or the salesperson. The trust of the buyer in the product/service will contribute to the knowledge of how important the functional trust influencers are for the buyer. The importance of these individual trust relationships will be discussed in Chapter 6.

Martucci et al. (2012) distinguished between "hard trust" and "soft trust" in cloud computing. They argued that the hard trust criteria make assumptions about the security, reliability and dependability of cloud services that can be assessed by audits, certificates and reports. However, from their point of view, hard trust criteria are "not necessarily sufficient for cloud consumers to trust cloud providers" (Martucci et al., 2012, p. 6). They argued that cloud computing also involves soft trust aspects such as individual experiences in the interaction between the parties, intrinsic human emotions and other factors such as brand loyalty. According to the authors, soft trust assumes that hard trust mechanisms are not perfect and that errors can always happen, even

with the most sophisticated technical arrangements. However, many of the studies on trust in cloud computing concentrate on the hard trust mechanisms and not on the soft trust properties (e.g. Roberts II and Al-Hamdani (2011)). The current research will aim at analysing the soft trust factors involved in the purchase decisions of the buyer by capturing the individual experiences the key informants had with cloud computing services, the reservations they have regarding U.S. cloud providers and the emotions involved in the matter of the surveillance activities of foreign governments. As outlined in Chapter 4, the best way of studying these soft trust factors is a qualitative research design including the appropriate data collection and analysis methods.

In 2013, Noor et al. (2013) conducted a review of the existing literature on trust management frameworks and prototypes. Three years later, in 2016, Noor et al. (2016) published an updated review of the existing literature and their framework for analysing trust management systems. The authors noted that there was a fair degree of variety in the reviewed research prototypes and that none of the existing frameworks did address all variables that are involved in managing trust in cloud computing. More recent trust management frameworks that were not analysed in these reviews were for example proposed by Chong, Abawajy, Ahmad, and Hamid (2014), Fan and Perros (2014), Manuel (2015), Chiregi and Navimipour (2016), Macías and Guitart (2016) and Varalakshmi and Judgi (2016).

However, all of these models were only based on artificial data and only tested in theoretical experiments. None of these studies was based on empirical data. Although these models may contribute to the theoretical understanding of trust systems they are of questionable value for real-life applications. The current study aims to contribute to this growing area of research by collecting data on trust in cloud computing through semi-structured key informant interviews. Therefore, the findings of this research should make an important contribution to the field of trust in cloud computing.

Perhaps the most serious weakness of these studies on trust management frameworks was that they were not interested in the reasons and origins of trust or distrust in the cloud services but only focused on measuring trust based on different indicators. The current study therefore provides an important opportunity to advance the understanding of the reasons behind buyers trusting or distrusting cloud services by conducting a qualitative research.

There are also some doctoral theses that addressed the subject of trust in cloud computing. The doctoral thesis of Ries (2009) focused on automated trust evaluation models in a ubiquitous computing world. The thesis of Almanea (2015) compared popular trust evaluation tools for cloud computing trust issues, assessed their usefulness and proposed a framework to assess cloud provider trustworthiness. And the topic of the thesis of Pawar (2015) was about designing and evaluating a trust model that considers different aspects of cloud providers and a cloud broker mediation layer with different modes of operation. However, none of these theses analysed the underlying reasons for trust or distrust in cloud computing.

As described above, cloud computing is a relatively recent technology. IT outsourcing can be seen as a predecessor of cloud computing and the interaction between IT outsourcing and trust has been studied for a longer period of time (Böhm, Leimeister, Riedl, & Krcmar, 2011). Outsourcing is a management practice that originated in the 1950s (Greaver, 1999), but it was not until the 1980s until the idea was largely adopted by organisations around the world (Hätönen & Eriksson, 2009; Lonsdale & Cox, 2000).

Lansing and Sunyaev (2016) found that only a few studies have investigated the impact of trust on cloud computing adoption and that the few existing studies focused primarily on IT outsourcing. The authors argued that cloud computing has a “dual nature of being a service provided by an organisation and an IT artefact” (Lansing & Sunyaev, 2016, p. 59). They reasoned that cloud computing could be seen as an evolution of IT outsourcing and therefore decided to review 43 empirical studies on trust in IT outsourcing and trust in IT artefacts. Based on the reviews they created a conceptual model that defines trust-building antecedents and provides a conceptual typology of constructs for trust in cloud services. Although their model intends to create a common ground for future research, it lacks empirical testing.

A large part of the literature on trust in IT outsourcing focused solely on outsourcing of professional services such as software development projects (e.g. Sabherwal (1999), J.-N. Lee and Choi (2011)) rather than outsourcing server infrastructure to a data centre managed by an IT outsourcing provider. These studies are therefore not relevant for the objectives of this research. Other studies on trust in IT outsourcing focused on associated aspects such as long-term relationships in IT outsourcing

(Kishore, Rao, Nam, Rajagopalan, & Chaudhury, 2003) and knowledge sharing (J.-N. Lee, Huynh, & Hirschheim, 2008).

Probably the most relevant study on IT outsourcing for this research was conducted by Qi and Chau (2013) who investigated the roles of interpersonal and interorganizational trust in IT outsourcing success. Their findings suggested that interpersonal trust played a more influential role than inter-organisational trust for the success of IT outsourcing projects and the willingness to share knowledge. The results are consistent with the findings of most of the studies about salesperson trust discussed in Section 3.4.2. However, the study did not include the trust in the IT outsourcing product/service as discussed in Section 3.4.3 but only focused on inter-organisational and interpersonal trust.

In summary, all the previously mentioned studies suffer from some limitations. Most of the papers focused on creating theoretical models to assess trust using parameters such as public customer ratings and reviews and contractual SLA agreements. Only a few studies were concerned with the reasons behind the trust or distrust between the parties and none of the reviewed literature addressed the trust relationship between German companies and U.S. cloud providers. Additionally, none of the publications addressed all the different trust relationships outlined in Section 3.4. Only one study on IT outsourcing covered the topic of interpersonal and inter-organisational trust but did not factor in product trust.

Having reviewed the existing literature on the relationships in buyer-seller trust and the literature on trust in cloud computing, the following sections will focus on the cultural difference between U.S. cloud providers and German companies.

3.6 The role of culture

Another objective of the current research is to analyse the impact of the cultural differences between Germany and the U.S. on the trust relationship between German companies and U.S. cloud providers. The following sections will review the current literature on the relationship between culture and trust, cultural differences between the U.S. and Germany and culture models in organisational research. The purpose of this literature review is to find concepts that explain differences in country culture and their effects on organisational behaviour.

3.6.1 Culture and trust

Today's globalised world of business and the worldwide transfer of capital, data and labour involve complex interdependencies within and between companies in different countries (Caldwell & Clapham, 2003; J. Child, 2001; Gulati & Sytch, 2008). And, although national cultural boundaries are becoming increasingly "fuzzy" in a globalised world (Doney, Cannon, & Mullen, 1998), the impact of national cultural characteristics on the values, beliefs and behaviours on people remains challenging for trust building (Dyer & Chu, 2000; J. L. Johnson & Cullen, 2002; Pothukuchi, Damanpour, Choi, Chen, & Park, 2002). This could also be said for public cloud services that are offered and consumed globally.

However, developing and maintaining trust between different cultures can be a difficult challenge (Dietz, Gillespie, & Chao, 2010). People from different cultures often have incompatible assumptions, "alien" values and beliefs and "peculiar" behaviours that can prevent fruitful and successful collaboration (e.g. Ariño, De la Torre, and Ring (2001); Branzei, Vertinsky, and Camp II (2007); Farris, Senner, and Butterfield (1973); Thompson (1996)). Therefore, cross-cultural interaction can lead to misunderstandings, embarrassment or psychological distress (Molinsky, 2007). The challenge of establishing, maintaining and repairing trust in cross-cultural settings might be most apparent across national borders (Dietz et al., 2010). For example, Ferrin and Gillespie (2010) analysed if the development, meaning and functions of trust differ between national-societal cultures and found evidence of cross-cultural differences in every category of their review.

Nevertheless, as claimed by Dietz et al. (2010), little is known about how people from different cultures understand the construct of trust and how they build, maintain and repair trust in their own culture and across cultures. Likewise, S. Zaheer and Zaheer (2006, p. 21) argued that researchers "have still barely begun to explore the related idea that trust may differ systematically across cultures". The authors maintained that culture determines what people find trustworthy and what they consider as foundational to trust (S. Zaheer & Zaheer, 2006). As suggested by Dietz et al. (2010), people with a shared cultural background, including the associated norms and values, should hold a common understanding about what is required to create and maintain trust. Since the "trust cues" are familiar to both parties, people with a common cultural

background might be more likely to build trust (Doney et al., 1998, p. 616) and might grow it faster (Griffith, Hu, & Jr, 2000).

However, when these parties are from different cultures, this “familiarity” might not be available (D Harrison McKnight, Cummings, & Chervany, 1998). The relationship between both parties could rather be described as a combination of dissimilar backgrounds, potentially mutual gain, and fear of being exploited (Dietz et al., 2010). According to Gibson, Maznevski, and Kirkman (2009), both parties give off cues about their trustworthiness and interpret the signals from these cues. Their own cultural filters (“schemas”) determine how these different cues are weighted and prioritized. This might lead to the situation where “cultural norms and values that are conducive to efficient trust production in one setting may be impotent, misleading and even damaging in another” (Branzei et al., 2007, p. 78). Likewise, Schwegler (2006) reasoned that, when one party is unfamiliar with the value system and cultural norms of their interaction partner, complications can emerge. Therefore, cultural differences are frequently attributed for being a barrier for building trust (A. Bird & Osland, 2005; Osland & Bird, 2000). As summarised by Dietz et al. (2010, p. 21), culture “influences the formation of trust cues in relationships, and serves as a filter for cues encountered from another culture”.

Seppänen et al. (2007, p. 252) also called “for more papers on cultural issues in inter-organisational research” to study the cultural and national implications in evaluating the concept of trust. According to the authors, only the studies of Sako and Helper (1998) and Dyer and Chu (2000, 2003) considered the cultural effect on trust. Their studies found that for example Japan, Korea and the USA have a diverse cultural understanding of the concept of trust. Other studies also found that trust is depending on one’s individual cultural background (Dasí-Rodríguez & Pardo-del-Val, 2015; Hewett & Bearden, 2001; Huff & Kelley, 2003; D. Y. Lee & Dawes, 2005; Leung, Lai, Chan, & Wong, 2005; Pirson, 2007; Uslaner, 2002; Young & Albaum, 2003). Dutton (2013, p. 277) argued that there was “a need for multifaceted research that will expand existing theories of trust in online environments by examining the role of culture” and other influential factors. Likewise, Schoorman, Mayer, and Davis (2007, p. 351) underlined the “potential value of future research to develop these links more carefully”. The impact of cultural differences between buyer and seller in the context

of trust in cloud computing services is therefore an interesting field for marketing research.

Having discussed the relationship between culture and trust, the following section will review the literature on cultural differences between the U.S. and Germany in areas such as personal information sharing, trust in institutions and trust in Internet service providers.

3.6.2 Cultural differences between Germany and the U.S.

In 1999, IBM commissioned a survey on consumers in the United States, Germany, and United Kingdom and their attitudes toward privacy in everyday business transactions (Harris Interactive, 1999). In terms of trust in a certain industry, only 10% of consumers in Germany had confidence in the abilities of Internet companies to secure their private data, whereas 21% of U.S. consumers were saying that they were somewhat confident. In comparison, 70% of German consumers and 77% of U.S. consumers trusted banks with their personal information. Overall, U.S. consumers had greater confidence than Germans in companies' handling of their private data in almost all industry sectors. However, the study commissioned by IBM is almost twenty years old and consumer behaviour might have changed within the last decades, especially in the area of Internet businesses and online shopping. The authors pointed out that, at the time of the survey, only 51% of the German respondents and 66% of U.S. respondents had access to the Internet. Additionally, the survey was conducted in a business-to-consumer (B2C) and not in a business-to-business (B2B) context such as the relationship between German companies and U.S. cloud providers.

In another study, H. P. Peters, Lang, Sawicka, and Hallman (2007) examined cross-cultural differences in public attitudes between Germany and the U.S. in the context of food biotechnology. In their analysis, the authors focused on three areas: trust in institutions, appreciation of nature and attitudes towards genetically modified food. Their results indicated that U.S. citizens had "significantly more institutional trust" than Germans, particularly in the "perceived intensions of political and economic institutions" (H. P. Peters et al., 2007, p. 205). The study also found that "appreciation of nature" was significantly lower in the U.S. than in Germany. Overall, in seven out of eight items of the attitude scale developed by H. P. Peters et al. (2007), U.S. respondents were significantly less critical or more positive about food biotechnology

than the German respondents. H. P. Peters et al. (2007) concluded that the lower appreciation of nature and the higher relevance of trust make the U.S. culture more receptive to assimilate technological innovations than the German culture. However, the question arises if this is the case for technology in general or only for technology which has a direct influence on nature. It could therefore be argued that e.g. cloud computing technology has only low influence on nature or even a positive influence compared to traditional data centres. This study was also conducted in a B2C context with citizens/consumers instead of business decision makers.

The study by L. R. Smith and Schwegler (2010) examined the trust-building processes in German and U.S. non-governmental organisations (NGOs) in international crisis areas. The authors identified trust as the “make-or-break factor” in international strategic partnerships and international humanitarian action. By applying the trust-building framework from Doney et al. (1998), L. R. Smith and Schwegler (2010) found a number of differences and similarities between German and U.S. cooperation development criteria. Regarding the “calculative process” defined by Doney et al. (1998), U.S. NGOs were looking for a return on invest (ROI) of their activities, whereas the German organisations highlighted long-term coalition building as one of their primary goals. From the point of view of L. R. Smith and Schwegler (2010), this result was not surprising because of the more individualistic national culture of the U.S. as described by Hofstede (2003a). Both, German and U.S. interviewees, had similar views on the “prediction process”. However, in many cases the NGOs interviewed in the study did not have sufficient prior experience with partner organisations to rely on this trust building process.

The “intentionality process” turned out to be a key trust process for both German and U.S. organisations. However, according to L. R. Smith and Schwegler (2010), the intentionality process for German organisations is more about integrity and benevolence in general and through a “code of conduct”, whereas the U.S. organisations were in search of a shared cultural identity that would provide a basis for resource sharing. The “capability process” only showed subtle differences between German and U.S. organisations. L. R. Smith and Schwegler (2010) found that the German NGOs were more pragmatic by citing expertise, competencies, capacities and resources as key decision factors for partnerships, whereas the U.S. respondents

stressed core competencies and potential synergies as important attributes of potential partners. In terms of the "transference process, both, German and U.S. NGOs, showed interest in the reputation of their potential partners. However, L. R. Smith and Schwegler (2010, p. 298) reported that German organisations would gather information about the reliability and reputation of potential partners through formal processes, whereas U.S. organisations would operate on a more "intuitive assessment of like-mindedness".

Overall, L. R. Smith and Schwegler (2010, p. 298) described the German organisations as being "more principle driven, rational and formal by relying on written reports and local consultants". The U.S. organisations, on the other hand, were characterised as being model driven and focusing on partnerships with like-minded organisations and practical benefits. However, the authors acknowledged that these were mostly subtle differences and that not all themes that emerged in the analysis could be captured by the cognitive trust-building processes defined by Doney et al. (1998). The study was conducted with NGOs specialised on humanitarian missions in crisis areas. It is therefore questionable if the results are applicable to enterprise organisations such as the U.S. cloud providers and German companies of the current research. Additionally, the authors focused upon the role of trust in international cooperation in crisis areas in general and the cultural differences between German and U.S. organisations were rather an example for different approaches than the focal point of this research.

A study conducted by Krasnova and Veltri (2010) explored the role of culture and the "privacy calculus" between U.S. and German social networking site users. The authors compared the behaviour and willingness to share personal information on the international social networking site Facebook. Krasnova and Veltri (2010) found that U.S. citizens were less worried about giving personal information to a U.S.-based social network site company and were more open to sharing their personal information on the Internet with other members of the social network site. The authors also found that U.S. citizens felt that they had more control of the information they shared, were better informed about the information handling procedures, had more trust in the legal systems protecting their privacy and had more trust in the social networking site itself. The German users, on the other hand, expected higher damage in case of negative

outcomes and perceived a higher likelihood of negative consequences. Additionally, the German users had a lower level of trust in the competence, honesty and benevolence of the U.S. social networking site.

Krasnova, Veltri, and Günther (2012, p. 129) compared their research results with the five cultural dimensions defined by Hofstede (2003a), which, in their opinion, “has received the widest acceptance” of all cultural frameworks. Both countries have low perception of power distance (PDI), are higher than average on the dimension of masculinity (MAS) and have low scores for long term orientation (LTO). Though, “both countries significantly differ” in their level of individualism (IDV) and uncertainty avoidance (UAI) (Krasnova & Veltri, 2010, p. 2). As highlighted in the discussion chapter, Hofstede (2018) updated the model by introducing a sixth dimension and changing the scores for the long-term orientation dimension. The study of Krasnova and Veltri (2010), however, is based in the dimensions and scores introduced by Hofstede (2003a).

While the U.S. has an IDV score of 91, the score for Germany is 67. The U.S. culture was described as having a strong self-orientation and an emphasis on hedonism and self-reliance whereas Germany “takes the form of a legal-bureaucratic orientation combining low economic individualism, low affective collectivism, and an emphasis on formal rules and categories” (Morris and Leung 2000, p. 112). With regard to UAI, the U.S has a score of 46 and the score for Germany is 65. The “much higher level” of UAI could signal “anxiety about the future, lower level of subjective well-being and willingness to take only the known risks” (Krasnova et al., 2012, p. 130).

The hypotheses of Krasnova et al. (2012), that the negative impact of privacy concerns on self-disclosure is stronger in uncertainty avoiding cultures than in uncertainty tolerant cultures, was supported. In other words, the authors found that Germany, as a culture with a higher UAI level, had more concerns about sharing private information. Another hypotheses, that the positive impact of trust in the social network services providers on self-disclosure is stronger in individualistic cultures than in collectivistic cultures, was also supported (Krasnova et al., 2012). This implies that more individualistic cultures such as the U.S. have more trust in social network services providers in handling their personal data than less individualistic countries such as Germany. These two outcomes might be of interest regarding the objectives of the

current research and the relationship between U.S. cloud providers and German companies.

However, the study by Krasnova et al. (2012) focused on students and not on business people. Although both groups might share similar values, the interests and regulatory requirements differ between the parties. While individuals can decide for themselves what personal data they are willing to share, companies are required to protect the personal identifiable information of their employees and customers in compliance with applicable laws. Additionally, the study was conducted in a time where the “VZ Netzwerke” had a large share in the German social network services market which makes it more difficult to compare with the U.S. social network service Facebook. Finally, Krasnova et al. (2012, p. 134) considered individuality and uncertainty avoidance to be “the sole cultural determinants behind the impact of trusting beliefs/ anticipated benefits and privacy concerns respectively”. Other trust dimensions were not studied in detail.

This section has analysed the literature on cultural differences between the U.S. and Germany. The following section will review the existing models of national culture and select a model for the current research.

3.6.3 Models of national culture

Culture has a strong influence on how people think and what they do (Tinsley, 1998). According to Smircich (1983), culture expresses the beliefs, values and ideas that group members share, facilitates commitment to a group and gives group members a sense of identity. Schein (2010, p. 29) maintains a similar view and argues that culture defines “what things mean, how to react emotionally to what is going on, and what actions to take in various kinds of situations”. Similarly, Gibson et al. (2009, p. 48) claim that culture “provides insight into how to be a person in the world, what makes for a good life, how to interact with others, and which aspects of situations require more attention and processing capacity”.

In their highly cited book on concepts and definitions of culture, Kroeber and Kluckhohn (1952) identified over 160 different definitions. Today, more than 60 years later, the definition of culture remains diverse and fragmented (Dietz et al., 2010). This also applies to the various existing models that try to capture and structure the

differences between cultures. According to Nardon and Steers (2009), there is a lack of convergence between models of national culture and researchers must choose between multiple and often conflicting, competing or overlapping models. Some of the most widely cited and utilised national culture models in organisational research include models proposed by Kluckhohn and Strodtbeck (1961), Hofstede (2003a), Hall (1990), Trompenaars (1993), Schwartz (1992) and House, Hanges, Javidan, Dorfman, and Gupta (2004).

Kluckhohn and Strodtbeck (1961) proposed a theory of culture based on value orientation which served as a foundation for several later models. The authors argued that, in any society, “values are distributed in a way that creates a dominant value system” (Nardon & Steers, 2009, p. 3). Kluckhohn and Strodtbeck (1961) identified five cultural dimensions (relationship with nature, relationship with people, human activities, relationship with time, human nature), each of which is represented in a three-point-continuum (e.g. future, present and past for “relationship with time”).

Hofstede (2003a) based his widely used model (Miltgen & Peyrat-Guillard, 2014) on the assumption that cultures can be distinguished based on what they value. From his point of view, one can gain substantial insight into cultural behaviour based on five dimensions (power distance, uncertainty avoidance, individualism-collectivism, masculinity-feminity, long-term vs. short-term). He created this model from studying employees from various countries working for multinational companies.

The model of Hall (1990) is based on three cultural dimensions (context, space and time). His research focused on how cultures vary in interpersonal communication, the extent to which people are comfortable with sharing personal space and how people manage their time (Nardon & Steers, 2009). Trompenaars (1993) based his model on his study of large corporations such as Shell over a period of ten years and focuses on relationships between people, time management, and the relationship between society and nature (Nardon & Steers, 2009). He created a model which consists of seven dimensions (universalism-particularism, individualism-collectivism, specific-diffuse, neutral-affective, achievement-ascription, time perspective, relationship with environment).

Schwartz (1992) identified three cultural dimensions (conservatism-autonomy, hierarchy-egalitarianism, and mastery-harmony) that “reflect the solutions that

societies find to regulate human actions" (Nardon & Steers, 2009, p. 6). His model has been applied to studying social groups but the application to studying organisations has been limited (Bond, 2001). Lastly, the international team around House et al. (2004) defined nine cultural dimensions (performance orientation, power distance, uncertainty avoidance, humane orientation, institutional collectivism, in-group collectivism, assertiveness, gender egalitarianism, future orientation) and collected data from 62 countries for their study. The researchers focused on studying the influence of cultural differences on "Global Leadership and Organisational Behaviour Effectiveness" (GLOBE) and created a detailed report on the different leadership styles they identified in these countries.

In their article on "the culture theory jungle", Nardon and Steers (2009, p. 20) compared these different models and concluded that all models have important factors that contribute to a better understanding of the relationship between culture and management practices. However, the cultural models focus on different aspects of norms, values and beliefs, which makes convergence across the models difficult. Additionally, some authors such as Hofstede (2003a) and House et al. (2004) created country-specific numeric scores for each of their cultural dimensions whereas other authors used qualitative descriptions.

Despite these differences, Nardon and Steers (2009) aimed to integrate and consolidate these models of national cultures into "core cultural dimensions" for reducing the "confusion caused by both the overlap and differences across models". By seeking common themes and principal cultural characteristics through their comparative analysis, Nardon and Steers (2009) defined five "core cultural dimensions" (hierarchy-equality, individualism-collectivism, mastery-harmony, monochronism-polychronism, universalism-particularism) and mapped them to country clusters, such as Anglo and Germanic. The intend of Nardon and Steers (2009, p. 19) was to "propose a vehicle for understanding cultural differences based on the previous work" of six researchers in that field. It could, however, be argued that, by consolidating existing models, Nardon and Steers (2009) created an additional model that competes with any existing model. The authors acknowledged that "any attempted integration" of existing models "obviously requires further study and validation" and that each of their core cultural dimensions "may lose its relevance or

even meaning when studied individually or out of context" (Nardon & Steers, 2009, p. 20). Ultimately, additional research was required to understand the relationship between cultural differences and management practice. However, according to Nardon and Steers (2009, p. 21), "accurate data in support of research will frequently be difficult to collect and analyse" and "researchers must rely on personal insight and intuition, reflection, and collaboration" to make progress in this field.

In contrast, Osland and Bird (2000) criticized and questioned the usefulness of pre-defined cultural categories and referred to them as "sophisticated stereotyping". In their opinion, the subtleties and complexities of national cultures, and the situational context and the individual background of the acting parties are neglected by applying these theoretical cultural dimensions (Wright & Ehnert, 2010). Osland and Bird (2000, p. 65) argued that, "since so many exceptions and qualifications to the stereotypes, on both a cultural and individual level, come to mind". Similarly, Wright and Ehnert (2010) argued that the notion of culture might be overemphasized and culture was instead one of several factors that influence human interaction.

Chao and Moon (2005) added an additional point of view. They reasoned that, when different cultures interact, a new hybrid culture is created which is unique to the particular context. The authors argued that at least one of the parties learns from the other, adapts to the situation and thereby changes the way both sides interact.

3.6.4 Hofstede's cultural dimensions

The current research will discuss the cultural themes from the interviews using Hofstede's cultural dimensions in the discussion chapter. According to Miltgen and Peyrat-Guillard (2014), Hofstede's model is one of the most popular conceptualisation of national culture and more than 60% of cross cultural studies use at least one Hofstedian dimension (Leidner & Kayworth, 2006). While multiple frameworks address cultural differences, the model of Hofstede has received the widest acceptance (Krasnova et al., 2012). Moreover, several studies on cross-cultural research (e.g. Milberg, Smith, and Burke (2000), Bellman, Johnson, Kobrin, and Lohse (2004), Dinev et al. (2006), Posey, Lowry, Roberts, and Ellis (2010)) confirmed that "the relationship between people's national culture and valuation of privacy reflect Hofstede's framework" (Miltgen & Peyrat-Guillard, 2014, p. 107). Since (data) privacy is one of the key topics of the current research, Hofstede's framework appears to be an

appropriate choice. Thus, the current research adopts the definition of national culture by Hofstede (1991, p. 5) as a “collective programming of the mind which distinguishes the members of one group or category of people from another”.

However, although the model of Hofstede is dominating national cultural research, his model of national culture has some limitations that research must address. As mentioned above, culture is in general difficult to define and conceptualise (Boyacigiller, Kleinberg, Phillips, & Sackmann, 2004) and it is even more challenging to establish a measure that can calculate the distance between dimensions of cultures (Shenkar, 2001). Critiques of Hosftede’s approach note that the theory might be too simplistic, that it might be too difficult to understand culture through numbers and that culture would not equate to nations (Baskerville, 2003; Ess & Sudweeks, 2005; D. P. Ford, Connelly, & Meister, 2003; Myers & Tan, 2003; H. J. Smith, Milberg, & Burke, 1996; Søndergaard, 1994; Straub, Loch, Evaristo, Karahanna, & Srite, 2002).

Despite the criticism, Hofstede’s model is widely used and many authors have demonstrated that his model functioned well for their research (Baskerville, 2003; Ess & Sudweeks, 2005). As argued by Miltgen and Peyrat-Guillard (2014), studies that have used alternative models of culture, such as the GLOBE framework, returned similar results. In response to his critiques, Hofstede (2003b, p. 811) explained that his second edition of Culture’s Consequences was “capitalizing on 20 years of applications of the ideas in the 1980 edition” and many details such as the number of dimensions and the scores have changed over time. Hofstede (2003b, p. 813) wrote that he sees his “work as exploratory research, not as a finished theory” and that he made an effort to formulate his conclusions in a “tentative and falsifiable way”.

Hence, the current research will discuss the cultural themes from the interviews using the Hofstede’s cultural dimensions and compare the results with previous studies. Figure 13 illustrates that, according to Hofstede (2018), the strongest differences between Germany and the U.S. can be found in the dimensions of individualism, uncertainty avoidance, long-term orientation and indulgence.

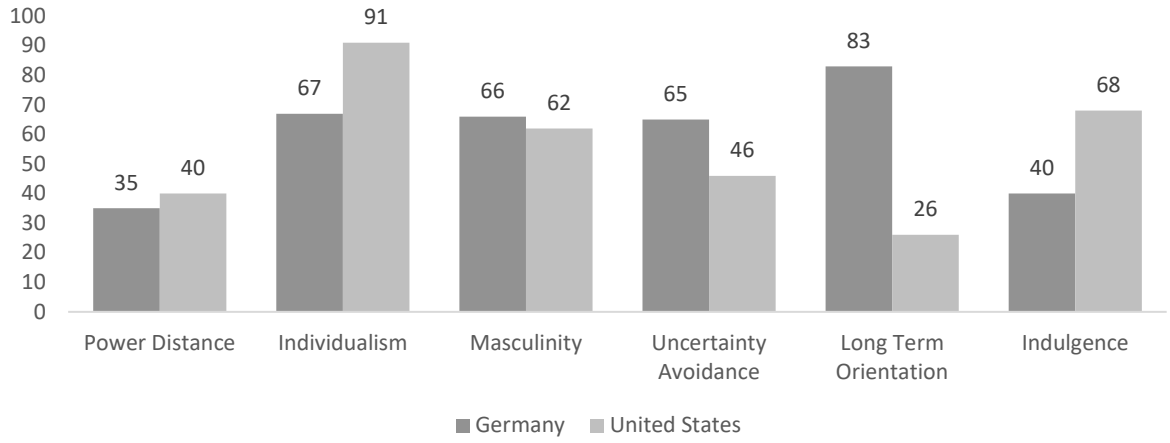


Figure 13: The six dimensions of national culture. Adapted from Hofstede (2018).

In comparison to the model applied by Krasnova and Veltri (2010) that was discussed above, Hofstede (2018) extended his dimensions of national culture with a sixth dimension named indulgence. In addition, Hofstede and Minkov (2010) changed the scores for the long-term orientation dimension from 31 to 83 for Germany and from 26 to 29 for the U.S. in comparison to the scores from Hofstede (2003a). According to Krasnova and Veltri (2010, p. 3), the long-term orientation dimension has been "consistently omitted from intercultural privacy-related studies", e.g. in Cao and Everard (2008) and Lukenbill (1999).

In previous studies, individualism and uncertainty avoidance have been identified as key influencer for trusting beliefs and the impact of privacy concerns (Krasnova et al., 2012). Additionally, in studies on electronic commerce, individualism played a central role in affecting the trusting beliefs in the platform providers (Lim, Leung, Sia, & Lee, 2004; Sia et al., 2009). Lim et al. (2004, p. 553) argued that "the interaction between individualism and uncertainty avoidance plays a dominant role in explaining Internet shopping rates across cultures". Greenfield (2000, pp. 229-230) even described the individualism vs. collectivism dimension as one of the "deep structures" and a "skeleton framework" of culture. Furthermore, Cao and Everard (2008) found a strong positive connection between uncertainty avoidance and privacy concerns for instant messaging users. Likewise, Dinev et al. (2006, p. 391) used Hofstede's individualism and uncertainty avoidance metric to "explain the differences in privacy concerns, perceived risk and trust between" the U.S. and Italy. Therefore, the discussion in

Chapter 6 will primarily focus on the dimensions of individualism and uncertainty avoidance but also include the dimensions of long-term orientation and indulgence.

The following section will analyse and summarize the gaps in the literature reviewed above and formulate the research objectives, which lays the foundation for this research.

3.7 Research gaps

So far, this chapter has focussed on the review of the existing literature in buyer-seller trust relationships in connection with cloud computing. This section will summarise the gaps identified in the literature and derive the research questions from these gaps and from the background information outlined in Chapter 2.

3.7.1 Importance of trust

As detailed in Chapter 2, German companies have a relatively low cloud computing adoption rate in comparison to other countries in Europe or to North America. Several practitioner studies have tried to find an explanation for the low adoption rate and explored the main concerns raised by German companies. However, as stated in the section above, there is no academic study on the trust relationship between German companies and U.S. cloud providers.

While much research is being conducted in the cloud computing technology itself, there is an urgent need for understanding the business-related issues (Marston et al., 2011). Several authors, e.g. S.M. Habib et al. (2010), Khajeh-Hosseini, Sommerville, and Sriram (2010), Kanwal et al. (2013) and Ullah and Xuefeng (2013) have identified the topic of trust in public cloud services as a research challenge. Additionally, to improve the security of cloud computing technologies, the European Union Agency for Network and Information Security ENISA (2009, p. 7) proposed further research in the areas of “building trust in the cloud” and “international differences in relevant regulations including data protection and privacy”. This study seeks to obtain data which will help to address these research gaps.

Impact of cultural differences

Knowledge about culture is critical in an interconnected, global world where people from different cultural and ethical backgrounds have to work together and form personal and professional relationships (Dinev et al., 2006). Hence, as argued by

Dinev et al. (2006, p. 397), validating models of information technology use “across cultures is of utmost importance for a globalized economy and further development and expansion of information systems and their use”. Previous studies have found that national culture affects the role and nature of trust (e.g. Dyer and Chu (2000), Sako (1992)). However, as argued by Seppänen et al. (2007, p. 251), the majority of the studies on trust in buyer-seller relationships were conducted at the national level in the U.S. and, therefore, there is a need for “more papers on cultural issues in inter-organizational research” on trust. Additionally, previous studies of intercultural trust in buyer-seller relationships have not dealt with cloud computing services as a new paradigm in information technology and international business.

This study aims to contribute to this growing area of research by exploring the cultural dimensions of trust between German companies and U.S. cloud providers from a dyadic perspective of buyers and sellers. This also includes the history and culture of Germany (see Section 2.1.5.1) and specific characteristics of the German economy (see Section 2.1.5.2).

Influence of the sector

To date there has been little agreement on the influence of the sector or industry a company is operating in on the adoption of public cloud services. More recently, literature has emerged that offers contradictory findings about the adoption of public cloud services by German companies with respect to the sector.

The issue has grown in importance in light of recent developments following the global surveillance disclosures. The debate about the influence of the sector on cloud adoption has gained fresh prominence with many arguing that the public sector and the financial services industry are particularly hesitant to adopting public cloud services. Furthermore, most studies on the influence of the sector have only been carried out by market research companies and practitioner publications.

The aim of this study is to shine new light on these debates through an examination of the views of the buyers of German companies and local sales representatives of U.S. cloud providers on the influence of the sector on public cloud adoption.

This gap in the literature leads to the first set of research question for this study:

- What are the perspective of the buyers and sellers on
    a) the importance of trust for German companies for the adoption of public cloud computing services from U.S. cloud providers (RO1a),
    b) the impact of the cultural differences between Germany and the U.S. on trust and public cloud adoption (RO1b) and
    c) the influence of the sector of a German company on trust and public cloud adoption (RO1c)?

This set of research question was addressed in multiple interview questions in the interview guide (see Section 4.4.4). The following section will address a research gap related to the relationships that exist in buyer-seller trust.

3.7.2 Trust relationships

Debate continues about the influence of the different sales relationships to the buyer. As shown in Section 3.4, within the literature of trust in buyer-seller relationships, there has been considerable research on the trust relationships between the buyer and the selling company, the buyer and the salesperson and the buyer and the product or service. Still, some authors argue that literature indicates that the field of buyer-seller trust is under-researched and requires more study (Evans, McFarland, Dietz, & Jaramillo, 2012; Friend et al., 2018). The current research adds to a growing body of literature on buyer-seller trust by addressing the following knowledge gaps in the field of study.

Company trust

The literature on trust in the selling company reviewed in Section 3.4.1 was mainly based on quantitative research. However, the main weakness of these studies is the failure to address how trust in the selling company is built and how it influences the purchase decision of the buyer. Although much is currently known about effect of company trust, the mechanism by which they influence buyer decision making has not been clearly established, especially in the context of U.S. public cloud services and German companies. Additionally, there is a need to explore how the trust in the company is impacted by external events such as the global surveillance activities. This includes the trust relationship between German buyers and U.S. cloud providers in

comparison to German cloud providers and the attitude of German buyers towards private cloud solutions in their own on-premise data centres.

Hence, this research examines the role of trust in the selling company in the context of U.S. cloud services and the impact of external forces such as the press coverage of the global surveillance disclosures.

Salesperson trust

As shown in Section 3.4.2, a number of studies found that the relationship with a salesperson has a significant influence on the purchase decision of the buyer. However, as argued by Guenzi and Georges (2010, p. 132), “there is a lack of empirical research specifically investigating the contribution of salespeople’s behaviours in fostering customer trust”. Additionally, although extensive research has been carried out on the influence of a salesperson on the purchase behaviour of a potential buyer, no single study exists which investigate the role of a local sales representative of a U.S. cloud provider in the context of selling public cloud services to German companies. Moreover, since cloud services can also be purchased online without salesperson interaction, it might be interesting to explore how this impacts the importance of the salesperson to German buyers. Furthermore, there is a need for additional research investigating the conditions under which adaptive selling techniques have a positive or negative impact on sales performance (e.g. Guenzi et al. (2016)).

Therefore, this thesis intends to determine the extent to which salespeople influence the trust of a German company buyer and whether the buyer relies upon the assistance of local sales representatives of U.S. cloud providers for purchasing public cloud services.

Product trust

As reviewed in Section 3.5, a large number of studies agree on the importance of trust for cloud computing adoption. However, far too little attention has been paid to the trust of German companies in the technology behind cloud computing in general and the technological capabilities of U.S. cloud providers in particular. What is not yet clear is the impact of the trust of the buyer in cloud computing technology on his or her purchase intentions of U.S. public cloud services. Although findings of recent market

research have shown that U.S. cloud services are superior to European or German products, no academic studies have been reported that asked buyers and sellers about their perspective. Additionally, while there has been much research on shadow IT cloud services in general, there has been little empirical research into the impact on the trust relationship between German companies and U.S. cloud providers.

This indicates a need to understand the various perceptions of trust in cloud computing services and technology that exist among German buyers and how the trust in the technology impacts the adoption of U.S. cloud services.

Foreign government trust

Research on the subject of buyer-seller trust relationships has been mostly restricted to comparisons of company trust, salesperson trust and product trust. However, the studies on trust in general and in cloud computing adoption in particular failed to take any further connections into account. The practitioner literature as outlined in the background chapter suggest that there is at least one additional relationship that plays a key role in the trust of German companies in U.S. cloud services. This additional trust relationship can be described as the “trust in a foreign government” or “foreign government trust”. In the case of the current research, the foreign government is represented by the U.S. government. So far, however, there has been little discussion about the influence of the foreign government on the trust of the buyer.

Although the foreign government (U.S. government) does not have a direct business relationship with the buyer (German company), the trust of the buyer in the foreign government might have an impact on the purchase decision of the buyer. As illustrated in Figure 14, the selling company (U.S. cloud provider) is subject to the legislation of the foreign government (U.S. government). Therefore, the foreign government has not only an influence on the selling company, but also on the product (public cloud service) of the selling company and the salespeople of the selling company.

This is even the case when the selling company, the product and the salesperson are all located in different countries. In case of this research, the headquarters of the selling companies is in the U.S., the product/service is in a data centre in a country of the EU (e.g. Ireland) and the salesperson has a local work contract in Germany.

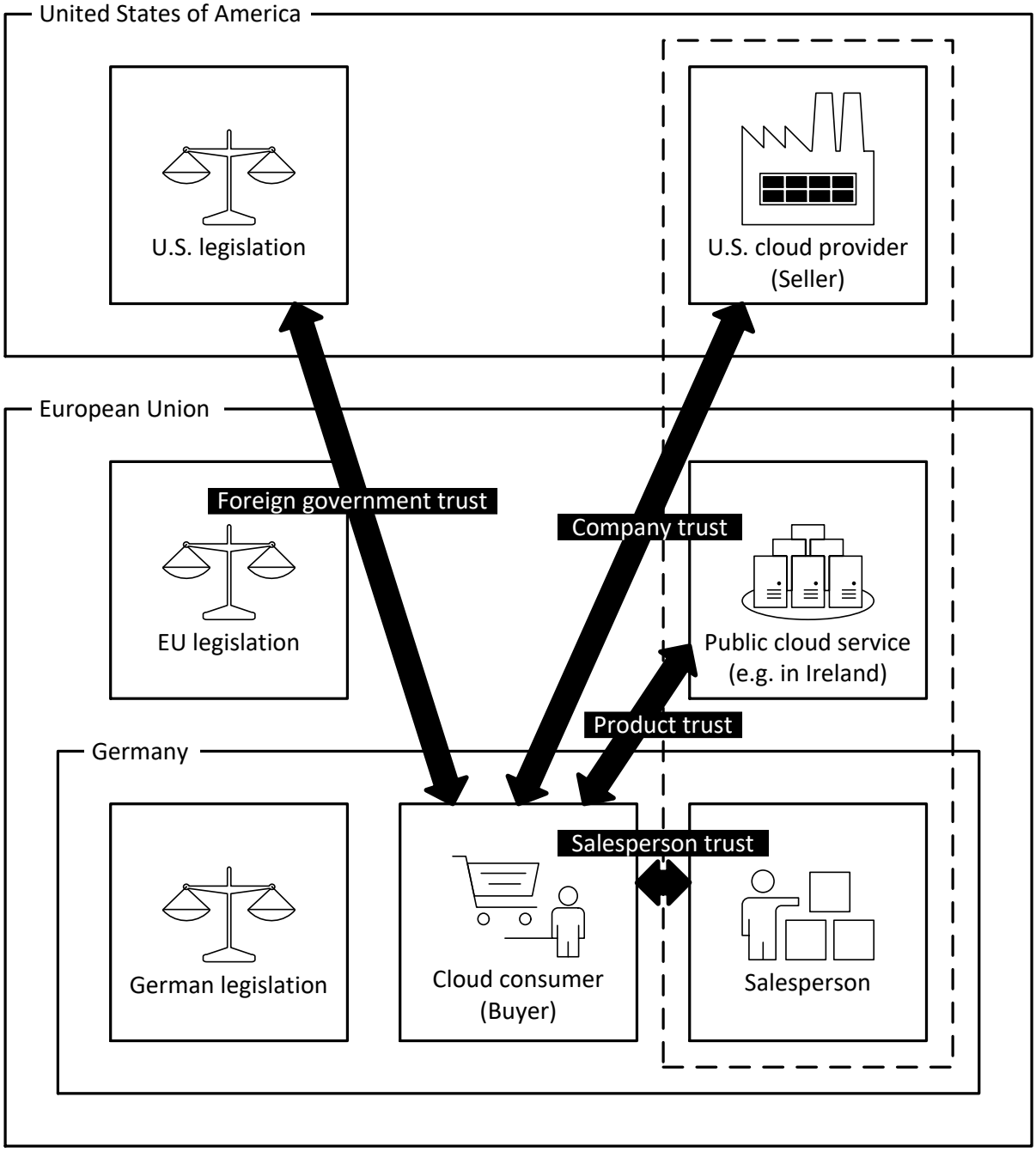


Figure 14: Foreign government trust

As discussed in Section 2.1.6.2, Germany has one of the most severe data privacy laws in the world whereas the U.S. has much less data privacy requirements. Therefore, the different and nested jurisdictions shown in Figure 14 can have a strong influence on the decision-making process of the buyer. Other studies also point in this direction. Research on buyer-seller trust in global business-to-business e-commerce found that geographical boundaries “still play important roles in economic agents’

attitudes, behaviours, and decisions" (Tat Koon Koh, Mark Fichman, & Robert E. Kraut, 2012, p. 904).

A recent study conducted by El-Gazzar et al. (2016, p. 72) on cloud computing adoption issues revealed that a main issue expressed by the interviewees was "related to clients' trust, involving the governments of countries that host the cloud environment". The authors argued that this concern was to some degree connected with the NSA surveillance revelations and that cloud consumers who were operating in the EU region would "prefer contracting EU-based CSPs rather than US-based international CSPs". El-Gazzar et al. (2016, p. 78) called the increased awareness of cloud consumers about the possible threats that foreign governments pose to data privacy the "Snowden effect" and concluded that the distrust in foreign governments "will influence cloud adoption decisions regarding the location of data storage". Kshetri (2013, p. 12) suggested that "future research might examine how political, ethical, social and cultural factors are associated with security issues in cloud computing". However, a review of the existing literature did not reveal any research on the impact of the U.S. government on the trust of German companies in U.S. cloud services.

It could be argued that international joint ventures pose similar trust challenges on companies. One example are foreign companies such as German car manufacturers investing in China to gain access to the Asian market. International joint ventures are a common vehicle for foreign market entry and approximately 320,000 collaborative ventures were established in China by the end of 2005 (Fang et al., 2008). Trust was identified as a critical factor in the success of collaborative ventures in China (Luo, 2000). However, a search for literature on the impact of trust in the Chinese government on the investment decision of foreign companies did not reveal any insights applicable to this research. This indicates a need to understand the various trust relationships that exist in this setting.

Hence, this thesis will examine the way in which the trust of the buyer in the foreign government influences his or her purchase behaviour and how this trust relationship impacts the relationship of the buyer with the selling company, the salesperson and the product or service. This leads to the second research question:

- How important is the trust relationship between German companies and
    a. U.S. cloud provider companies,

b. the local sales representatives of the U.S. cloud provider companies,
c. U.S. cloud products/services and
d. the U.S. government?

This research question was approached in multiple interview questions in the interview guide (see Section 4.4.4). Having addressed the contributions of this research to knowledge, the following section will focus on the managerial impact of this study.

3.7.3 How U.S. cloud providers can improve the trust in their services

As outlined above, cloud computing is a major paradigm shift in information technology and a multi-billion-pound business. While the market of cloud computing services is growing rapidly, it is difficult for cloud consumers to identity trustworthy cloud providers; and service level agreements (SLAs) are not sufficient to rate the trustworthiness of a cloud service provider (Sheikh Mahbub Habib, Ries, Mühlhäuser, & Varikkattu, 2014). As shown in Section 3.5, a number of researchers have reportet that trust is an influential factor for public cloud computing adoption. Hence, practitioners, and especially U.S. cloud providers, should be interested in how they can improve the trust of their customers, in this case German companies, in their cloud services. As stated by Abbadi and Alawneh (2012), trust establishment in cloud computing requires collaborative efforts from academia and industry. Uusitalo et al. (2010, p. 719) argued that future research should focus on “trust affectors, to better understand how to build cloud services” that cloud consumers trust. Additionally, Chiregi and Navimipour (2017, p. 21) stated that analysing trust characteristics such as integrity, security, availability, reliability, dependability, safety, dynamicity, confidentiality and scalability in cloud computing are “interesting lines for future research and work”.

However, none of the studies reviewed for this research have asked German companies how U.S. cloud providers could advance their services in order to improve the trust of German companies in U.S. cloud services. This thesis will examine the way in which U.S. cloud providers can improve trust and cloud adoption from the perspectives of German buyers and the local sales representatives of the U.S. cloud providers.

This study will address this gap in the literature with the following third research question:

- How can U.S. cloud providers improve the trust relationship with German companies?

The corresponding interview questions can be found in the research guide in Section 4.4.4.

3.8 Summary

Trust is a complex, multi-dimensional concept that can be studied in an almost infinite number of ways and in various academic disciplines. Although most authors agree on the importance of trust for humanity and also in commercial settings, the precise nature of trust, however, has yet to be fully explicated.

There is a great amount of practitioner literature and surveys which ask for the concerns of German companies regarding U.S. cloud services. However, only a few publications focused on the notion of trust as a determining factor for cloud service adoption and a review of the current academic literature did not reveal any study addressing the importance of the concept of trust for German companies for the adoption of cloud services from U.S. providers. In addition, there is a need to analyse the impact of the cultural differences between the U.S. and Germany and the sector or industry a company is working in on trust and the adoption of U.S. cloud services. The first research question of this study will try to contribute to the body of knowledge in this area.

To date, studies concerned with buyer-seller trust relationships have aligned roughly in three groups: studies that analyse inter-organisational trust in general, studies that recognise the role of the salesperson in buyer-seller trust and studies that also take the product or service as a third trust relationship variable in to account. However, there is a need to study these relationships in regard to the trust of German companies in U.S. cloud services. Moreover, in contrast to the first three forms of relationships, little conceptual work or research focuses on the trust in a foreign government and its influence on the other trust relationships. This lack of attention will be addressed in the second research question of the current study.

The third research question is aiming at the managerial impact of this study and is trying to answer the question how U.S. cloud providers could raise the trust of German companies in their cloud services. A review of the current literature did not reveal any scholarly work on the subject.

This chapter has demonstrated that, although extensive research has been carried out on buyer-seller trust, no single empirical study exists which explores the trust relationships in buyer-seller trust between German companies and U.S. cloud providers. The literature review chapter also identified several gaps in the current literature and derived the research questions that guide the following steps of this study. It is now necessary to explain the course of the data collection and analysis for the current research. The next chapter of this thesis will outline and justify the research design applied for this study.

4 Research design

The design of this study is based on the research aim and objectives, as well as a review of relevant literature, and is organised in the following way (see Figure 15). The chapter begins with the selection of the research paradigm, a justification for the appropriate research methodology and an explanation for the choice of the central research method.

The subsequent section explains the procedures for collecting the data for this study including the selection and recruitment of the research participants. Section 4.5 gives details on the data analysis and coding procedures applied in this study.

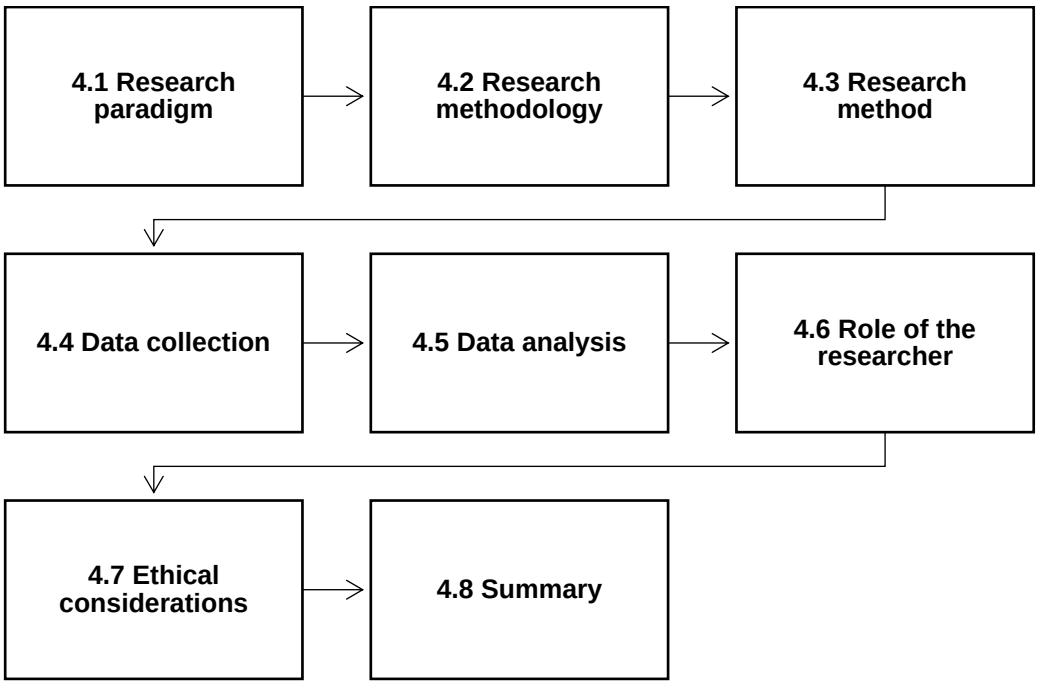


Figure 15: Research design chapter

Thereafter the role of the researcher in the context of this study is discussed which is followed by the ethical considerations that were made.

The last section summarises the key aspects of the overall research design including the choice of the methodology and method of this study.

4.1 Research paradigm

Research is guided by a set of beliefs or worldviews known as paradigms (Killam, 2013). The choice of the research paradigm has a strong impact on the research project. It contains important assumptions about the way the world is perceived, which give the researcher a platform for the research strategy (H. Collins, 2010). It is therefore central to understand the paradigm that supports the "decisions to be made in staking a research position" (Carson, 2001, p. 1) and to help researchers to identify which research design works best for their individual research (Easterby-Smith, Thorpe, & Lowe, 2002). Paradigms are "world views" which, in the individual context of a scientific domain, facilitate research and study activities (Edgar & Sedgwick, 2008) and are more a philosophy than a methodology, which guides researchers in their way of thinking about and conducting their research (Gliner & Morgan, 2000).

However, paradigms "cannot be proven or disproven" (Guba, 1990, p. 18) and "one cannot declare an alternative-paradigm view correct and another incorrect in any absolute sense" (Gioia & Pitre, 1990, p. 598). Paradigms are human constructions and therefore subject to human errors (Guba & Lincoln, 1994). There is a wide variety of different research paradigms in literature which often have different labels for the same paradigm. These include positivism, post-positivism, critical theory/transformative pragmatism and constructivism. The paradigm for the current research is constructivism, which will be explained in the following section.

4.1.1 Constructivism

The constructivism paradigm is based on a relativist ontology and is the most contrasting paradigm to positivism (Killam, 2013). Constructivists believe that reality is socially constructed (Alvesson & Sköldberg, 2009) and cannot exist without context (Killam, 2013). Therefore, each person has their own reality, which is influenced by social interactions and experiences (Guba & Lincoln, 1994). Consequently, people can have multiple socially constructed realities that are equally correct (Mertens, 2014), may conflict with each other (Guba & Lincoln, 1994), and can change over time (Killam, 2013). The research participants and the researcher are seen as co-creators of the research findings (Killam, 2013). The researcher's voice is that of the "passionate participant" who is "actively engaged in facilitating the multi-voice reconstruction" of the constructions of all participants as well as of himself/herself (Guba & Lincoln, 1994,

p. 115). A consensus is reached through continuous comparing and contrasting of findings (Killam, 2013). The researcher and the object of investigation are therefore interactively linked and findings are “literally created as the investigation proceeds” (Guba & Lincoln, 1994, p. 111).

Guba and Lincoln (1994, p. 107) define paradigms as “basic belief systems based on ontological, epistemological and methodological assumptions”. For constructivists, “there is no alternative but to take a position of relativism” as their ontology (Guba, 1990, p. 26). From their point of view, reality is socially constructed and multiple constructions can be apprehended and be in conflict with each other (Mertens, 2014). In this sense, “constructivism means that human beings do not find or discover knowledge so much as construct or make it” (Schwandt, 2000, p. 197).

Epistemologically, constructivists take a subjectivist position (Guba, 1990). The investigator and the object of investigation are connected in an interactive process where each side influences the other (Mertens, 2014) so that “the findings are literally created as the investigation proceeds” (Guba & Lincoln, 1994, p. 111).

The methodologies used by constructivists are based on the interactions between the researcher and the research participants (Killam, 2013). Hence, qualitative methods such as interviews are predominant in this paradigm (Mertens, 2014). The constructivist aims to identify the variation of constructions and to “bring them into as much consensus as possible” (Guba, 1990, p. 26). These “individual constructions” are “interpreted using conventional hermeneutical techniques” and “compared and contrasted through a dialectical interchange” (Guba & Lincoln, 1994, p. 111). This approach ensures that multiple perspectives are obtained to yield better interpretations of meanings (hermeneutics) which are contrasted and compared through a (dialectical) interchange comparing previous and sometimes conflicting ideas (Mertens, 2014).

4.1.2 Justification

As with every research paradigm, there is no “right answer” to the best philosophical approach (Easton, 2010, p. 128). However, because of the following reasons, constructivism is the preferred and most suitable paradigm for the current research.

Firstly, the objectives of this research require an exploratory and qualitative approach, which is in line with the constructivist worldview. For example, the first research question asks how important the concept of trust is for German companies for the adoption of public cloud computing services from U.S. cloud providers, which requires qualitative research methods. Secondly, social constructivists “focus on the specific contexts in which people live and work in order to understand the historical and cultural settings of the participants” (Creswell, 2013, p. 8). A key element of the current research is the cultural difference between U.S. cloud providers and German companies and the historical background of both parties. And thirdly, this research involves a dynamic interaction with the research participants and a deep inquiry into the participant’s view of the situation being studied. Constructivists recognise that their own “personal, cultural and historical experiences” shape the interpretations of the research (Creswell, 2013, p. 8), which is a position I agree with because it corresponds with my personal world view.

Constructivism is a common research tradition to the study of business networks and business-to-business marketing problems (L. D. Peters, Pressey, Vanharanta, & Johnston, 2013) and a “useful methodological frame of reference” in strategic management research (Mir & Watson, 2000, p. 950). Since business to business networks “in the real world are, largely, a reflection of the researchers' knowledge and understanding of them” (L. D. Peters et al., 2013, p. 345), constructivism is well suited for this kind of enquiry.

Constructivism is also a widespread paradigm in the field of trust research. Constructivist perspectives add a “significant dimension to our understanding of the trust-building process by drawing attention to the realities and subtleties of the social interactions through which trust or trustworthiness may emerge” (Murphy, 2006, p. 434). In a constructivist approach, trust is viewed as an active force in a relationship or network which helps to “mediate, shape and construct that very relationship or network” (Vosselman & Van der Meer-Kooistra, 2009, p. 268).

Wright and Ehnert (2010, p. 124) argued that cross-cultural trust emerges in a context that is not fixed and “to understand better how actors create trusting relationships a social constructionist perspective is needed”. The authors named three reasons why trusting across cultural contexts should be analysed from a social constructivist view:

First, trust is a narrative process that is created through a social process of conversation and interaction. Therefore, studying cross-cultural trust requires that researchers become part of the research setting, carefully listening to and holding conversations, and being aware of their role as a researcher. Second, trust should be seen as an emerging, ongoing, and endless process of "trust-in-the-making" and researchers should keep in mind that the thought processes and conversations of actors are shaped by their historical experiences. However, this interplay of past, present and future may differ between people and social settings. Third, all social phenomena, including trusting, are socially constructed and cross-cultural trusting takes place within settings that are continuously evolving. Hence, researchers should develop insights into how trusting is practiced and how this shapes their actions. It could also be argued that "trust research itself is a social construction constituted by scholars who have developed a way of speaking about trust that has become normalized" (Wright & Ehnert, 2010, p. 124).

Even in a field like information systems that is traditionally dominated by a positivist paradigm, the adoption of constructivist principles adds recognised value (Chiasson, Henfridsson, Karsten, & DeGross, 2011; Kaplan, Truex, Wastell, Wood-Harper, & DeGross, 2006; Willcocks, Sauer, & Lacity, 2016). The constructivist paradigm should hence be a suitable approach for cloud computing research.

Since, in constructivism, the research participants and the researcher are seen as co-creators of the research findings, it is important to address the fact that I am employed at a U.S. cloud provider. The implications for the current research will be discussed in Section 4.6 "Role of the researcher".

The following sections on the research methodology, research method, data collection and data analysis will demonstrate how a constructivist research position was applied in the current study.

4.2 Research methodology

Having defined the paradigm for the current research, it is now necessary to select an appropriate research methodology. The choice of any research methodology should be derived from the research paradigm (Bryman & Bell, 2011), as well as from the nature of the research questions and objectives (Flick, 2014). Sapsford (2006, p. 175)

defines methodology as “the philosophy of methods” and the “worldview that underlies and informs a style of research”. This view is also supported by Clough and Nutbrown (2012, p. 31), who argue that “the task for a methodology is to explain and justify the particular methods used in a given study”. This research will consider qualitative research as a methodology while the more practical application will be described as methods. The three major research methodologies are quantitative, mixed methods and qualitative research. The following section will highlight the qualitative research as the methodology of choice for the current research.

4.2.1 Qualitative research

Qualitative research is a “broad approach to the study of social phenomena” (C. Marshall & Rossman, 2010, p. 3) and uses a range of different methods to interpret social processes in a particular context (Jupp, 2006). The qualitative research approach takes place in a natural setting (Denzin & Lincoln, 2011), draws on multiple interactive and humanistic methods, focuses on context, is constantly developing and evolving, and is fundamentally interpretive (C. Marshall & Rossman, 2010).

It is hence a methodology that sees social reality as a “constantly shifting emergent property of individual’s creation” (Bryman & Bell, 2011, p. 27). According to qualitative researchers such as Guba and Lincoln (1994, p. 106), human behaviour cannot be understood without the purposes and meanings “attached by human actors to their activities” and only qualitative research can provide these “rich insights”.

4.2.2 Justification

This is, for the following reasons, also in line with the nature of this study. Firstly, since the paradigm of the current research is constructivism, a qualitative inquiry is particularly suited (Klenke, 2008). In contrast with a positivistic-quantitative approach, the qualitative researcher “honours an inductive style, a focus on individual meaning, and the importance of rendering the complexity of a situation” (Creswell, 2013, p. 4).

Secondly, one of the key findings of the literature review was that the research on trust relationships in business to business settings was mainly based on quantitative studies. As summarised by Wright and Ehnert (2010, p. 119), “the dominant discourse among trust researchers is positivistic”. Hence, to make a contribution to the body of knowledge, the current study will apply a qualitative research methodology. Moreover,

as described in the literature review, the reviewed studies did not agree on a common method to quantify trust and the research results could not be directly compared, replicated and validated. Additionally, the objectives of the current research, such as to identify ways how U.S. cloud providers can improve the trust relationship with German companies, require qualitative research methods.

And thirdly, as suggested by Seppänen et al. (2007, p. 261), “due to the fact that the concept of trust is apparently not easily quantifiable, it seems obvious that qualitative empirical studies and piloting are also called for before quantitative surveys are carried out”. Consequently, with regards to the research objectives, the qualitative research methodology is the best approach for this research.

4.3 Research method

As explained in the previous section, a qualitative research approach is particularly well suited for the constructivism research paradigm and the objectives of the current research. The purpose of this section is to select and justify an appropriate research method for this study.

Research methods are also called “research designs” Creswell (2013, p. 12) or “strategies of inquiry” (Denzin & Lincoln, 2011, p. 243) which “describes the skills, assumptions, enactments, and material practices that researchers-as-mythological-bricoleurs use when they move from a paradigm and a research design to the collection of empirical materials” (Denzin & Lincoln, 2011, p. 246). However, no research method is inherently superior or inferior to any other, and the choice of the method should be determined by the specific task at hand and guided by the individual research topic, questions and objectives (Saunders, Lewis, & Thornhill, 2009; Silverman, 2009, 2013).

The main methods for collecting qualitative data are observations, document reviews, focus groups and individual interviews (Creswell, 2013). The advantage of observations is that researchers can record information as it occurs and that it allows exploring topics that may be uncomfortable for participants to discuss. However, it would be difficult to get the permission and also time consuming to follow several IT managers and cloud sellers over a long period of time to answer the research questions about trust in U.S. cloud services. Document reviews enable researchers to

obtain insights from large data sets without direct interaction with respondents. This approach would, however, require access to sensitive information such as meeting minutes and emails from IT managers and cloud sellers discussing topics such as IT strategy and supplier trust.

Focus groups are useful to obtain detailed information about opinions, perceptions and feelings of a group of people on the same topic. They use group dynamics to generate qualitative data and can save time and money compared to individual interviews. However, as described in the sections on data collection, it was already difficult to get access to individual key informants for interviews and it would have been even more challenging if not impossible to agree on a time for a group of people from each organisation.

Therefore, the selected research method for the current study is qualitative interviews which will be discussed in more detail in the following sections.

4.3.1 Qualitative interviews

Qualitative interviews is the most popular data collection method in qualitative research (Cassell & Symon, 2004; J. Harding, 2013). They yield qualitative data quickly (C. Marshall & Rossman, 2010) and provide essential insights into human affairs and behavioural events (Yin, 2009). In contrast to quantitative structured surveys where the researcher tries to minimise inter-personal communication with the interviewee, the relationship is part of the qualitative research process and the respondent is seen as an active participant of the research (Cassell & Symon, 2004). On the downside, as mentioned above, qualitative interviews are more resource intensive and time consuming than quantitative methods and lack the naturalistic properties of observation and the possibility to study the collective understandings offered by focus groups (J. Harding, 2013).

4.3.2 Justification

For the following reasons, qualitative interviews are the most suitable research method for the current research. Firstly, the aim of this research is to explore the trust relationship between German companies and U.S. cloud providers. The objective of any qualitative interview is to investigate the research topic from the point of view of the interviewee and to find out why and how they have this specific perspective

(Bryman & Bell, 2007; Cassell & Symon, 2004). Qualitative interviews are therefore particularly helpful to examine how people such as the German IT managers make decisions, to study their beliefs and perceptions, to determine the motivation for a certain behaviour and to gather information on sensitive issues (Hennink, Hutter, & Bailey, 2010; Silverman, 2013).

Secondly, the constructivist research paradigm encourages researchers to play an active role in the research process. The qualitative interviews method does not only allow the researcher to listen to the experiences and views of respondents for an extended period of time (DiCicco-Bloom & Crabtree, 2006) but also gives the researcher the opportunity to ask additional probing questions during the interviews to explore concepts further (J. Harding, 2013; Saunders et al., 2009). As maintained by Wright and Ehnert (2010), primary data in cross-cultural trust research are best understood as a co-construction between researcher and subject. According to the authors, interviews are a process where knowledge is co-constructed between two or more parties and where the questions and answers of both sides influence each other. Put simply, “interviews are social exchanges, not talking questionnaires” (Wright & Ehnert, 2010, p. 123).

Thirdly, the nature of this research is a sensitive topic requiring contribution from senior business executives. Qualitative interviews allow to collect in-depth factual and emotional data in a conversational mode and ensures that the respondents pay full attention to the topic (Bryman & Bell, 2007; Easterby-Smith, Thorpe, & Jackson, 2008; J. A. Maxwell, 2005).

Most qualitative research interviews have the following characteristics in common: the majority of the interview questions are open questions, the interviews have a low degree of structure and they focus on specific situations in the world of the respondent (Cassell & Symon, 2004). As detailed in the following sections, this is very much in line with the interviewing approach used in the current research.

4.4 Data collection

As recommended by T. Gao et al. (2005) and Ashnai et al. (2016), research on buyer-seller relationships should focus on the collection of dyadic data and include the perspectives of both the buyers and the sellers. However, according to Ashnai et al.

(2016), most current buyer-seller relationship studies are based on monadic data. Hence, the data collection for the current research includes both parties. The following sections will provide additional details on the application of the data collection process that was based on qualitative, semi-structured key informant interviews.

4.4.1 Key informants

One of the first descriptions of key informant interviews technique was published by Tremblay (1957) in his manual about field research (M. N. Marshall, 1996). Key informant interviews provide an approach to gather qualitative data when the underlying theoretical framework is not well understood (Cowles, Kiecker, & Little, 2002) by making one or more respondents a major source of information (Wolcott, 2008). The key informant interviewing approach is a variant of the general interviewing techniques with the particularity that the interview is conducted with a relatively small number of informants (Klandermans & Staggenborg, 2002) who have a specialised knowledge or expertise and are willing to share this with the interviewer (McKernan & James, 2013).

Key informants provide deep insights and detailed information about what is going on in their environment due to their position or personal skills (M. N. Marshall, 1996). They can be seen as “ideal informants in a study” and may be chosen because of their ability and willingness to cooperate and communicate (Neergaard & Ulhøi, 2007, p. 265) and because they have the necessary knowledge to give insightful answers that are often not available through a randomised design (McKernan & James, 2013). Therefore, key informant interviews give the researcher “otherwise unobtainable views” (Charmaz, 2014, p. 23), provide information and insight directly from knowledgeable people and are particularly useful to better understand a certain behaviour, attitude or motivation (USAID, 1996), such as the trust of German companies in U.S. cloud providers.

Since trust is a “soft concept” in terms of its measurement, the assessment of trust relies on personal judgments that is often based on interviews from carefully selected respondents (Seppänen et al., 2007). All of the studies on inter-organisational trust reviewed by Seppänen et al. (2007) had a single key informant per company and the current research is following the same approach. Key informant interviews are also a useful instrument in research about internet business (Cowles et al., 2002), which

might also apply for cloud computing business relationships. Another advantage of the key informant technique is that it allows to collect a high amount of information and insights in a relatively short period of time (M. N. Marshall, 1996). Since time is a scarce resource which “has sharp boundaries and moves quickly for busy elites” (Charmaz, 2014, p. 72), key informant interviews are particularly suitable for busy business executives such as the IT managers of the German companies and the local sales representatives of the U.S. cloud providers.

A potential weakness of the technique is that the key informants are unlikely to represent the view of all members of their community (M. N. Marshall, 1996). For this reason, the key informants of this study were from different companies and represented different industries. Additionally, the group of interview participants was extended by local sales representatives of the U.S. cloud providers in Germany to get a more diverse view on the matter. Another limitation of this technique can be seen in the ability of a single key informant to speak for an entire organisation. However, the key informants in the current research have specialised knowledge and experience and are in a position that allows them to speak on behalf of their part of the organisation.

The amount of guidance provided by the interviewer can vary from unstructured non-directive to entirely structured interviews (Bryman & Bell, 2007). For key informant interviews, it is best to use a semi-structured interview format which allows the respondent to give answers in the way they see fit (Gofton & Ness, 1997). The following section will examine the use of semi-structured and open-ended questions in more detail.

4.4.2 Semi-structured and open-ended questions

Semi-structured interviews are not only the most appropriate approach for key informant interviews but also for the paradigm and method of this research. From a constructivist perspective, people construct meanings “as they engage with the world they are interpreting” and qualitative researchers therefore favour semi-structured interviews with open-ended interview questions to allow participants to share their views about a matter (Creswell, 2013, p. 9). One-to-one semi-structured interviews have become the “gold standard” and the most used qualitative research approach (Barbour, 2013, p. 111).

In semi-structured interviews, the interviewer has a framework of questions in mind and gives the respondent some orientation at the beginning of the interview (Tremblay, 1957). A key strength of semi-structured interviews is that it is extremely flexible (Easton, 2010). Questions posed to respondents are loosely structured (Cowles et al., 2002) and the researcher does not have ‘‘a specific set of questions that must be asked in particular words and in a particular order’’ (Babbie, 1998, p. 290). Since semi-structured interviews are not fully structured, interviewees can answer the question in a way that suits them best and to issues that interest them most (Greener, 2008). This flexibility in the form and order of the questions makes the interview more enjoyable for both parties and creates a more natural atmosphere (Greener, 2008).

Semi-structured interviews with open-ended questions allow a free flow of information, ideas and the emergence of unexpected insights (Gubrium & Holstein, 2002). The researcher can therefore take full advantage of those unanticipated topics and issues that open up during the interview (Gofton & Ness, 1997). The semi-structured interview technique is self-developing because the interviewer can refine his/her method during an interview and from one interview to another, as s/he gains more knowledge about the research topic and collects new ideas with each respondent (Tremblay, 1957).

In order to sustain and revive the interest of the informant in the topic, the interviewer can also follow clues and ask clarification questions (Tremblay, 1957). Questions should be asked where they fit naturally or may be raised by the interviewees themselves (Cassell & Symon, 2004). And, in case the answers of the informant are irrelevant to the topic, the interviewer can interject questions to bring the informant back on track without forcing the respondent to adopt a predetermined conversation pattern (Tremblay, 1957).

The practical application of the semi-structured and open-ended interviews approach on the interview guide including examples will be explained in Section 4.4.4. However, this technique also requires a number of different skills from the researcher (Seidman, 2006) which are discussed in the following section.

4.4.3 Interview skills

For conducting semi-structured interviews, the researcher needs to carry out several simultaneous tasks during the interview process, such as following his/her own line of

inquiry, asking the interview questions in an unbiased way, listening to the answers, taking notes, filtering and interpreting information and deciding about the next questions to be asked (Yin, 2009). The researcher should be, at the same time, structuring and open, gentle and critical, as well as knowledgeable and interpreting (Bryman & Bell, 2007). Keeping the dialogue with the interviewee flowing can be extremely tiring (Hackley, 2003) and requires a number of different skills from the interviewer.

Firstly, the researcher needs to be skilful at different forms of social interaction such as excellent listening and question framing skills (C. Marshall & Rossman, 2010). For that reason the researcher must use appropriate language and be prepared for dealing with difficult participants (Saunders et al., 2009). My professional work experience in various roles such as consulting, and sales was helpful with these three interviewing skills areas. Since I was used to have business conversations with business and IT managers, interviews felt natural and had a good flow. Nevertheless, since professional business conversations are not the same as academic interviews, I had to constantly reflect on and improve my interview skills with each interview session. For example, I had to make sure that the research objectives were addressed in the interviews but, at the same time, give the interviewees the freedom to talk about the topics they considered most interesting for the conversation.

Secondly, the researcher needs to be flexible and adaptive and be able to see newly encountered situations as opportunities and not as threats (Yin, 2009). Cassell and Symon (2004) even claim that flexibility during the interview process is the single most important skill for qualitative interviewing. Having prepared an interview guide helped me to jump between the questions and topics without losing track of what we had discussed already and what questions were still open. This gave me the flexibility required to follow up on new and unexpected issues and return to the prepared questions when most suitable.

And thirdly, interviewing key informants such as professionals or other power holders “with a higher status than oneself” requires a great deal of preparation and confidence (Burton, 2000, p. 225). As pointed out by M. N. Marshall (1996), the difference in status between the respondent and the interviewer can result in uncomfortable situations for both parties. Hence the researcher needs to be professional and assured and the

informant needs to feel that the researcher is a highly competent expert and that what they are saying in the interview is important (Gofton & Ness, 1997). My professional background in IT and specialised knowledge in cloud computing technologies helped me with having insightful conversations with the IT managers and the cloud sellers, ask the right questions and put their answers in the right context.

As described above, it was helpful to produce an interview guide which I could bring to all interviews. The following section will describe the creation of this guide.

4.4.4 Interview guide

Following the recommendation of J. A. Maxwell (2005), an interview guide based on the research question and objectives was created. The main purpose of the guide was to ensure that all required topics were covered. However, as described above, the interviewer does not need to discuss the topics in a certain order (Cassell & Symon, 2004) but rather use the guide as a checklist so as not to miss out an important subject (Kvale, 1996). The guideline for the interviews for this research was to allow the respondents a substantial amount of freedom within the boundaries of the general research topic. And although the same broad topics were covered by each interview, I maintained the ability for the respondents to explore areas in depth which were of special significance for them. According to Schein (1985), events are considered as critical when the research participants themselves see them as such. This was, for example, the case when Buyer03 talked about how younger people were more open to modern technologies including public cloud services.

N. King and Horrocks (2010) argue that the interview guide can either include full questions or just include short phrases or keywords. The interview questions for the current research have been prewritten in proper sentence form, although they have rarely been asked this way during the interviews. The advantage of writing down full questions in the interview guide is that “it forces the researcher to think carefully about question formulation” (N. King & Horrocks, 2010, p. 38). The development of the interview questions listed in Appendix 1: “Interview questions” was based on the research questions and objectives developed in Section 3.7. The table includes a column which references the research questions to the corresponding research objective.

During the interviews, probes or probing questions were used to help answering the research questions and to give the interview a more natural flow. Those probes have the purpose to show that the interviewer is actively listening, to encourage the respondent to provider more detail on a topic, to give the respondent the possibility to express feelings and opinions, and to provide greater clarity in areas that require more detail (J. Harding, 2013). Furthermore, according to Cassell and Symon (2004), it is recommended to open the interview with a question that can easily be answered by the respondent without any distress or embarrassment. This has been addressed at the beginning of the interviews with general questions about the company and role of the respondent, for example: “How would you describe your role in your organisation?”.

Cassell and Symon (2004) also recommend that more sensitive and tough questions should be asked later during the interview after the respondent feel comfortable with the situation and both parties get to know each other. Therefore, most of the questions directly addressing the research objectives were asked in the second half of the interview. One example of the more difficult questions was: “How would you in particular assess the risks of economic espionage by using U.S. public cloud services?”.

The interview guide also took additional recommendations by Cassell and Symon (2004) into account. These recommendations include that leading questions that impose the researcher’s opinion on the respondent must be avoided, that the researcher needs to be careful of assuming that certain questions do not need to be asked because the answer seems to be obvious, and not to have several different questions in one single sentence that are separated by an “and” as a divider, but to separate questions into separate sentences instead. Additionally, at the end of each interview, I asked the respondents for any pieces of information that they felt were relevant for the research and that were not explicitly asked during the interview: “Is there anything that I might have forgotten to ask or anything that you would like to add?”.

The following section will cover the sampling process and the selection of the interview participants.

4.4.5 Interview participants

Since it is not possible to study “everyone everywhere doing everything”, sampling in qualitative research is as important as in quantitative research (Punch, 2009, p. 162) and a key issue for any kind of research (Silverman & Marvasti, 2008). In qualitative research, sampling is the thoughtful selection of the participants most appropriate for the study (Lewis-Beck, Bryman, & Liao, 2004) and is used to find, choose and access the relevant primary data sources from which research data will be generated (Mason, 2002). With qualitative research interviews, the research question determines who to interview, how many interviews are needed, the particular industry to be investigated and the type of required respondents (business managers, technical experts, opinion leaders, etc.) (Kolb, 2008).

Bell (2005) suggested that cooperation can be improved by arousing the interest of respondents in the research topic and offering a summary of the study findings. However, although all participants in the current study had a general interest in the final outcomes of the research, this was not the primary reason for them to agree to participate in the study. It seems that their relationship with my personal and professional network was a more important criterion for them to agree to being interviewed.

Gubrium and Holstein (2002) stated that it is necessary to give the respondents a choice of times and to keep the interview as short as possible. In fact, most of the scheduled meetings had been rescheduled by the participants many times since giving an interview to a student had a very low priority in their busy calendars. However, as pointed out by Charmaz (2014, p. 61), “people often enjoy helping a student”. This was also my experience with many of the respondents. And although these interviews had a relatively low priority for them, most participants seemed to have enjoyed the conversations.

It therefore required patience and flexibility until the actual interviews took place. According to Marschan-Piekkari and Welch (2004), the venue needs to be chosen wisely to minimise inconvenience for the respondent. Schmidt and Hollensen (2006) suggested that a viable alternative to the respondent’s workplace could be a quiet café close to the office building or to book a meeting room to reduce distractions and

interruptions. All respondents from the German companies preferred to be interviewed in their own office or a meeting room.

However, most of the respondents from the U.S. cloud providers preferred a telephone interview. As explained by Coldwell and Herbst (2004), on-site face to face interviews are comparably time-consuming and costly. Nevertheless, there are some limitations regarding the use of body language with telephone interviews on both sides (Beall, 2010). In general, personal face to face interviews involve a much stronger engagement with the respondents (Sarstedt & Mooi, 2011). To minimise traveling costs and to be more flexible, it was also considered to use video calls (e.g. Skype) to substitute a classic face to face meeting. However, the respondents chose to either have an on-site meeting or a telephone conversation.

The following sections will describe the selection and recruiting process of the respondents for the German cloud consumer companies (buyer) and the U.S. cloud provider companies (seller).

4.4.5.1 Interviews with German cloud consumer companies

The interviewees of the German companies had to meet certain criteria. One criterion was that the company needed to be a large-sized business. As the key informants of this study are IT managers (see Section 4.4.1), the organisation had to include the position of a CIO or equivalent IT manager. Some SMEs have IT manager positions and some SMEs are technological companies themselves with deep knowledge about information technology products and services. However, since this is not always the case for small and medium enterprises (SMEs), only large companies were included in this research. According to the European Commission, all companies with more than 250 employees are considered large enterprises (European Commission, 2015c). All companies interviewed in this research had more than 400 employees.

Another criterion was that those large enterprises were registered in Germany because they needed to be subject to the German law and legal system. However, the companies might operate only in Germany or have international offices worldwide, including the United States. This criterion was important because of the legal aspects for German companies which store and process data in a data centre of a U.S. cloud

provider. All companies interviewed for the current research had their headquarters in Germany and most of the companies had offices and subsidiaries outside of Germany.

Since cloud computing usage in Germany was considered relatively similar between different sectors or industries (see Section 2.1.5), the current research was sector-independent and did not take into consideration the characteristics of each individual industry. However, two sectors have been excluded from the research. One exception was the public sector because of governmental policies regarding the use of public cloud computing. A second exception were companies which were cloud service providers or resellers themselves, such as large telecommunications companies and IT service providers. Those sectors were therefore not included in this research.

According to Saunders et al. (2009), the ability to obtain suitable primary data depends on the researcher's access to an appropriate source and it can be very challenging to recruit busy senior executives for key informant interviews (Gratton & Jones, 2004). Flick et al. (2007) suggest that it is helpful to look for particularly typical cases and to choose those that are the easiest to access under the given conditions. The logical subsequent step is to identify the accessible population, which are persons the researcher has access to (Cooper, 1984).

My first attempt was to contact potential candidates through social networks for professionals such as LinkedIn and XING. However, I did not receive any reply to my messages. I assume that most people in those positions had already too many work and private engagements and had no time for additional commitments. Additionally, not all members of social networks like LinkedIn and XING are active users and it is easy to ignore or forget messages from unknown contacts.

Therefore, I changed my strategy and turned to my private network for help. Fortunately, my friends and (ex-)colleagues knew several potential interview participants and asked them if they would agree to be interviewed by me. When they accepted the request, I sent them an email to formally introduce myself and explain my research. Additionally, I set up a short phone call with each candidate to answer potential questions they had before the interviews and to schedule an appointment. Appendix 2: "Participant recruitment" shows the original message to the potential candidates on XING and LinkedIn, an example of the introduction email I wrote to the

contacts introduced by friends and (ex-)colleagues and a list of topics for the phone conversations.

As can be seen from Table 20, the key informants for the current study were eleven IT managers or Chief Information Officers (CIOs) from ten different German companies. People in those positions typically have the most comprehensive knowledge of their companies' IT setup as well as of the latest trends on the IT market. Additionally, managers have "the formal authority to prescribe interpretations" and their viewpoints can be "highly significant and instrumental" (Isabella, 1990, p. 10). Their experiences and opinions can therefore have a significant impact on the mindset of the organisation regarding the utilisation of U.S. public cloud services.

Table 20: Interviews with German companies

Respondent	Organisation	Industry	Language	Mode	Length
Buyer01	Company01	Insurance	German	On site	71 min
Buyer02	Company02	Advertising	German	On site	35 min
Buyer03	Company03	Conglomerate	German	On site	47 min
Buyer04	Company04	Manufacturing	German	On site	44 min
Buyer05	Company05	Electric utility	German	On site	38 min
Buyer06	Company06	Banking	German	On site	45 min
Buyer07	Company07	Insurance	German	On site	56 min
Buyer08	Company08	Industrial equipment	German	On site	69 min
Buyer09	Company09	Entertainment	German	On site	68 min
Buyer10	Company10	Logistics	English	On site	36 min
Buyer11	Company10	Logistics	English	On site	45 min

Most of the interviews were conducted in German and the interviews had an average length of 50 minutes. The last two interviewees came from the same organisation (Company10), where one person was the IT manager of a large division of the company and the other person was the head of the group IT. Both respondents were not German and had different nationalities. It was therefore interesting to hear their view on the German attitude towards U.S. cloud services. Their opinions will be discussed in the findings and discussion chapter.

With approval of the respondents, all conversations have been digitally audio recorded for subsequent transcription. All interview participants of the German companies were male which made it impossible to study any gender-specific issues.

4.4.5.2 Interviews with U.S. cloud provider companies

One selection criterion for the interview respondents of the U.S. cloud provider was that these companies had to have their headquarters in the USA. This criterion was important because these companies needed to be subject to the U.S. law and legal system which has further implications on their international business.

A second criterion was that these companies were selling enterprise cloud services and not only offer consumer cloud services. Many cloud service providers mainly target the consumer market. This research, however, required respondents from companies which had a strong portfolio of enterprise cloud services. Another criterion was that the U.S. cloud provider companies needed to have dedicated salespeople for the German enterprise market. Only sellers who were involved with selling U.S. cloud solutions to German companies could talk about their experiences.

As set out in Table 21, the interview respondents came from five different U.S. cloud provider companies which offered a mix of different enterprise cloud. Most interviews were conducted by phone. Unfortunately, none of the interview respondents agreed on audio-recording the interviews. Therefore, I had to take notes and use these notes for the data analysis.

Table 21: Interviews with U.S. cloud providers

Respondent	Organisation	Service(s)	Language	Mode	Length
Seller01	Provider01	IaaS, PaaS	German	Phone	77 min
Seller02	Provider02	SaaS	German	Phone	63 min
Seller03	Provider03	SaaS	German	Phone	91 min
Seller04	Provider02	SaaS	German	Phone	60 min
Seller05	Provider03	SaaS	German	Phone	55 min
Seller06	Provider04	IaaS, PaaS, SaaS	German	Phone	50 min
Seller07	Provider05	SaaS	English	On site	61 min
Seller08	Provider05	IaaS, PaaS	English	Phone	57 min

Most of the respondents from the U.S. cloud providers were recruited through my personal and professional network and some of the interviewees were contacted via professional social network platforms such as LinkedIn and XING. One of the cloud providers listed above was my current employer. The ethical implications of this relationship are discussed in Section 4.7.

4.4.5.3 Sample size

In any qualitative research, the sample size is never large enough to apply statistical reasoning (Easton, 2010). However, several researchers have anyway taken a positivist position and recommended a specific number of cases to be used. Eisenhardt (1989, p. 545) suggested that, “while there is no ideal number of cases, a number between 4 and 10 cases usually works well”. In their analysis of qualitative research interviews, Guest, Bunce, and Johnson (2006, p. 59) found that “saturation occurred within the first twelve interviews, although basic elements for meta-themes were present as early as six interviews”. And in a review of 14 publications on sampling and cases in qualitative research, S. E. Baker and Edwards (2012, p. 2) found that the response from most contributors to the question of “how many interviews is enough” was “it depends”. A larger number of respondents, on the other hand, does not guarantee the credibility of a study (Cassell & Symon, 2004).

B. Czarniawska (2014, p. 145) proposes that, “when your field material (interviews, observations, documents collected) becomes repetitive, it is time to stop”. Likewise, Ragin (in S. E. Baker & Edwards, 2012, p. 34) advises that “you should stop adding cases when you are no longer learning anything new”. This view is also shared by Bryman and Bell (2011), Flamez, Lenz, Balkin, and Smith (2017), Monsen and Van Horn (2007) and Saunders et al. (2009), who argue that saturation is reached when results get redundant or repetitive and additional interviews fail to provide new insights.

For the current research, saturation was reached after 11 interviews with buyers and 8 interviews with sellers. For both groups, the last two interviews did not add any significant insights. This resulted in a total number of 19 interviews with cloud consumers and cloud providers.

The current study specifically addressed IT managers as decision makers for cloud computing adoption. The main reason for choosing IT managers as key informants for this study was that they were considered to have the most comprehensive knowledge of their companies’ IT setup as well as being informed of the latest trends on the IT market. However, future studies could focus on the business decision makers of companies and analyse the trust of non-IT departments in public cloud services. Additionally, due to practical reasons, not all perspectives that could have provided additional insights were taken into account through primary data. For example, the

perspectives of German cloud providers and politicians from the U.S., the EU and Germany were only incorporated in an indirect and passive way through practitioner literature and the statements of the buyers and sellers. These gaps provide additional opportunities for future research.

4.4.6 Pilot interview

The phrasing of the interview questions and the way that the questions are asked during the interview process have a major influence on the usefulness of the responses (Cassell & Symon, 2004). A pilot interview can help improving the overall interview process because it can identify potential problems (J. Harding, 2013), is an excellent opportunity to check if the interview guide works as intended (Rose, Spinks, & Canhoto, 2014) and gives the interviewer the chance to refine his/her agenda and get some additional practice at conducting the interviews (Hackley, 2003). However, as argued by van Teijlingen and Vanora (2002), conducting a pilot interview does not guarantee success in the research study but it does increase the likelihood of success.

One of the initial tasks for setting up a pilot interview is the selection of the first interviewee. According to Yin (2009), the main criteria for the selection of pilot cases are usually geographic proximity, access and convenience (Yin, 2009). Another important criteria is to select a person who is representative for the people to be interviewed later (Gillham, 2000). This was also the case with the pilot interview of this research which was conducted with Company01 (see Table 20). Buyer01 was open to the idea to be the first participant and gave additional feedback to the interview procedure.

Pilot interviews help refining data collection plans (Yin, 2009), help estimating the length of an interview (Sampson, 2004) and are crucial for trying out the interview questions (Merriam, 2014). The researcher learns which questions might be confusing and need rephrasing, which questions generate answers that are not very useful for the study and what questions were not in the interview guide but should have been in there (J. Harding, 2013; Merriam, 2014). For the current research, the lessons learned from the pilot interview regarding field and research procedures have been incorporated into the design for the following interviews. However, not many changes were necessary. The amount and complexity of the questions met the estimated timeframe of about 60 minutes for the interview.

Nevertheless, some of the questions have been slightly rephrased and additional questions have been added. The “version” column in Appendix 1: “Interview questions” show which questions were part of the original set of questions, and which questions have been added after the pilot interview. One example of a question that was not part of the original set of questions but was included after the pilot interview was about the impact of the German culture and history on the adoption of U.S. cloud services. Since the interviews with the sales representatives of the U.S. cloud providers (sellers) only started after the completion of all interviews with the buyers, and because the questions for the sellers were very similar to the questions for the buyers, I assumed that there was no need to test the interview questions in another pilot. This assumption turned out to be correct and the interviews with the sellers went as good as with the buyers.

Moreover, pilot interviews can also serve further purposes such as getting started with the interview process, practicing asking questions and active listening, and getting feedback on the method and content of the interview (Griffee, 2005). It is therefore highly recommend that at least one pilot interview is conducted with a member of the sampling group (Rowley, 2012). In case of the current research, the pilot interview helped me to test and improve my interview skills discussed in Section 4.4.3. Overall, the conversation had a good flow and the respondent was happy to tell about his personal background, experiences, opinions and suggestions. The interview atmosphere was professional and friendly, and the interviewee gave depth and comprehensive answers to the interview questions.

Having described the data collection procedures for the current research, the following sections will focus on the analysis of the interview data.

4.5 Data analysis

There is no “one right way” to interpret qualitative data and all decisions of how to analyse a dataset are unavoidably subjective (Auerbach & Silverstein, 2003, p. 32). After reviewing the literature on qualitative data analysis, thematic analysis was selected as a suitable method for the current research.

Thematic analysis can be defined as “a method for identifying, analysing and reporting patterns (themes) within data” (Braun & Clarke, 2006, p. 79). It can be “widely used

across a range of epistemologies and research questions" and is a "highly flexible approach that can be modified for the needs of many studies, providing a rich and detailed, yet complex account of data" (Nowell, Norris, White, & Moules, 2017, p. 2).

Accordign to Guest, MacQueen, and Namey (2011), the thematic analysis researcher has the choice between three analytical approaches: exploratory analysis, explanatory analysis and confirmatory analysis. The current research follows the exploratory, "classic content-driven, inductive approach" which emphasises "on what emerges from the interaction between researcher and respondent" (Guest et al., 2011, p. 36). For example, as explained in the sections on data collection, I rarely asked the interview questions the way I formulated them in the interview guide but rather asked questions in an interactive and conversational style to give the talk a natural flow. Some interviewees also asked questions back for clarification or because they were themselves interested in my experience and opinion on technical and organisational issues. In these cases, I had to politely steer the conversation back to the respondent's views on the research questions. Thus, the content of the interaction between the interviewer and interviewee drove the development of the themes which is in line with the constructivist paradigm applied to this research.

The data analysis of this research was supported by the computer software Nvivo for Windows. The use of computer software for research analysis has many advantages such as with handling large volumes of data, searching and statistical functionalities, computer-aided development of consistent coding schemes and help with sampling decisions (Greener, 2008; N. King & Horrocks, 2010; Silverman & Marvasti, 2008). However, although computer software can be helpful to organise large amounts of data, it is not capable of the intellectual process of transforming data and making any kind of judgement (N. King, 2004). It was therefore my task to decide about what codes to focus on, how to collect additional data and, most importantly, how to interpret the data. From my experience, the software was particularly helpful with sorting and merging codes and building a code hierarchy.

Braun and Clarke (2006) suggested six different phases of thematic analysis. The current research adopted the following techniques based on these standard thematic analysis phases. Although the thematic analysis process will be presented in a linear

way, it is actually a reflective and iterative process that can jump between the phases and develops over time (Nowell et al., 2017).

4.5.1 Transcription

The first phase involves transcribing the data collected during the interviews, reading and re-reading the data and noting down initial ideas (Braun & Clarke, 2006). All interviews with cloud consumers (Buyer01-Buyer11) were recorded using a professional digital audio recorder. Afterwards, these interviews were transcribed by me in the original language of the interview without external help. As suggested by Greener (2008), this approach allows the researcher to hear all interviews a second time during transcription and to get to know the interviews in great detail. Some researchers even argue that this should be seen as a a key phase of data analysis (C. M. Bird, 2005; Lapadat & Lindsay, 1999; Riessman, 1993). All spoken words were transcribed except for a few filler words such as “uh” and “um” and some mistakes that the respondents corrected themselves while talking. The transcripts have not been checked by the interviewees after transcription, but they were checked against the recording during the coding process. All transcribing work was carried out using the transcription module of NVivo for Windows. In addition to the recordings, I took notes during and after the interview about personal impressions, body language of the interviewee and the atmosphere during the interview.

As described above, none of the cloud sellers gave the permission for recording the interview. I therefore took notes during the interviews to capture as much as possible of the answers of the respondents. According to Oppenheim (2000), the disadvantages of taking notes instead of using audio recordings are that the researcher is not able to capture everything that has been said and that respondents may become distracted by the note taking process. Furthermore, recording the exact words of respondents allows to use direct quotes in the research findings and is a requirement for certain data analysis techniques (J. Harding, 2013). Fortunately I was able to capture a few direct quotes from the cloud sellers in my notes. N. King and Horrocks (2010) suggest that if it is not possible to record the interview, details should be added to the notes directly after the interview because the conversation is still fresh in the mind of the researcher. Following this recommendation, I complemented the

interview notes directly after the interview with what has been said by the respondents but has not been written down during the interview.

As suggested by Braun and Clarke (2006, p. 87), in preparation for the initial coding, I went through the process of “repeated reading” of the data in an “active way” and started to take notes of initial ideas that came up during the reading process. During the course of the current research, I recorded general thoughts as well as more detailed coding ideas in Microsoft OneNote. Those notes often started as a simple drafting of thoughts and ideas and grew in accuracy, complexity and density as the data analysis progressed. Appendix 3: “Coding and notes writing” provides an example of these notes.

4.5.2 Generating initial codes

The second phase involves the generation of initial codes from the data. Codes “identify a feature of the data (semantic content or latent) that appears interesting to the analyst” (Braun & Clarke, 2006, p. 88) and are “the most basic segment, or element, of the raw data or information that can be assessed in a meaningful way regarding the phenomenon” (Boyatzis, 1998, p. 63). Codes differ from the units of analysis (themes), which are (often) broader (Braun & Clarke, 2006). The themes are developed in the next phase and are the basis for the interpretative analysis of the data in relation to the phenomenon being examined (Boyatzis, 1998). Coding can be performed either for the entire data set or only for certain parts. I followed the recommendation of Braun and Clarke (2006) to work systematically through the entire data set by giving equal attention to each data element and identifying interesting aspects that could form repeated patterns (themes).

I stopped interviewing after the first nine interviews and started analysing the data. As stated in Section 4.4.5.3, after I assumed saturation, I conducted two additional interviews with buyers to confirm my assumption. For these two and all following interviews with cloud sellers, I engaged in simultaneous collection and analysis of data.

There are a number of different ways to perform the actual coding process including handwritten notes, highlighters, coloured pens, post-it notes and by using computer software (Braun & Clarke, 2006). As described above, I used software tools for the

data analysis phase. Many qualitative researchers, especially in grounded theory, apply line-by-line coding to their data (Charmaz, 2014; Corbin & Strauss, 2014). Since the software which I used for the transcribing and coding process, NVivo for Windows, does not provide any “lines” to code, coding was performed for segments of data. These segments were one or several sentences that had a logic connection and could be coded with the same name. This approach follows the recommendation of Braun and Clarke (2006, p. 89) to “code for as many potential themes/patterns as possible” but, at the same time, “code extracts of data inclusively” and “keep a little of the surrounding data” to save the context. Appendix 3: “Coding and notes writing” provides an example of the coding process in NVivo for Windows.

4.5.3 Searching for themes

The third phase re-focuses the analysis on a broader level and involves sorting the codes into potential themes. The different codes are combined to form overarching themes and the relevant coded data extracts are collated within the identified themes (Braun & Clarke, 2006). A theme can be defined as “an abstract entity that brings meaning and identity to a recurrent experience and its variant manifestations. As such, a theme captures and unifies the nature or basis of the experience into a meaningful whole” (DeSantis & Ugarriza, 2000, p. 362). Moreover, themes are not dependent on quantifiable measures but rather on the question if they capture something important in relation to the overall research objectives (Braun & Clarke, 2006).

As explained by Nowell et al. (2017), some of these themes match an interview question whereas others are formed inductively and can form either main themes or subthemes. For example, the interview question “How would you in particular assess the risks of economic espionage by using U.S. public cloud services?” directly matches the theme “Economic espionage”. Other questions, such as “What do you think U.S. public cloud providers could do to improve the trust German companies have in their cloud services?” led to several themes such as “Data centre location” and “Data encryption”. Other themes such as “Shadow IT” were not directly linked to an interview question.

This process can be supported by visual tools such as tables, mind-maps and post-it notes. I used a combination of drawings, post-it notes and code hierarchies in Nvivo. Appendix 3: “Coding and notes writing” shows the code hierarchy created in Nvivo and

the development and naming of themes using slips of paper. Some of the initial codes developed to main themes, whereas others formed either sub-themes or were put under the identified themes. For example, “Shadow IT” developed to a main theme, while “Bring your own device” was placed as a sub-theme to “Shadow IT”. Not all codes were grouped into sub-themes and some codes remained directly under the main themes.

The collection of candidate themes and sub-themes was the foundation for the reviewing phase, detailed in the following section.

4.5.4 Reviewing themes

During this phase, the candidate themes will be examined if they need to be refined, combined, separated or discarded. This phase reveals inadequacies in the initial coding and may require changes to the candidate themes (N. King, 2004). Some themes may not really be themes because there is not enough data to support them and other themes may need to be merged together because there is no good reason to keep them separated (Braun & Clarke, 2006). The researcher may also find additional relevant issues in the data that need to be covered by a new code (Nowell et al., 2017).

I reviewed the collated extract of all candidate themes to see if they appeared to form a coherent pattern. If this was not the case, I had to either consider if the theme itself was problematic or if the data extract did not fit to the theme. Consequently, I had to either create a new theme, modify the theme or link the data extract to a different theme. For example, under the main theme “Sector and size”, there was a number of sub-themes such as “Enterprise”, “SME”, and “Sector” where different codes could be combined to form overarching themes. Other codes such as “Start-ups cannot do business without cloud” did not match the “SME” theme but needed to be moved to a separate sub-theme “Start-ups”.

This process of coding and re-coding needs to be continued until the thematic map “accurately reflects the meanings evident in the data set as a whole” (Braun & Clarke, 2006, p. 91). Following the advice of Braun and Clarke (2006, p. 92), I stopped the revision cycles after additional refinements were “not adding anything substantial” to the research.

4.5.5 Defining and naming themes

This phase involves defining and further refining the themes that will be used for presenting the analysis. Braun and Clarke (2006) explain “define and refine” as “identifying the essence of what each theme is about (as well as the themes overall), and determining what aspect of the data each theme captures”.

Themes should not be too diverse and complex and should fit in the broader overall story in relation to the research questions and objectives. The names of the theses should be “concise, punchy, and immediately give the reader a sense of what the theme is about” (Braun & Clarke, 2006, p. 93). N. King (2004, p. 263) advised that the list of themes cannot be considered final “if there remain any sections of text which are clearly relevant to the research question but remain uncoded”. Table 22 lists the themes defined for the current research after the data analysis of all texts including a short description.

Table 22: List of themes

No.	Name	Description
01	Importance of trust	Participant opinions about the importance of trust for cloud computing adoption
02	Culture and history	Influence of the history and cultural differences between the U.S. and Germany on cloud computing adoption
03	Sector and size	Influence of the sector and size of German companies on cloud computing adoption
04	Cloud computing technology	Participant opinion on the importance and maturity of cloud computing technologies for German businesses
05	U.S. cloud providers	Participant opinion on the features, performance and quality of U.S. public cloud services
06	Shadow IT	Prevalence and risk of shadow IT cloud services in German companies
07	U.S. cloud providers	Perception of the trustworthiness of U.S. cloud providers and their role in the global surveillance activities
08	German cloud providers	Reactions of German cloud providers to the global surveillance disclosures
09	Private cloud	Perception and adoption of private cloud services by German companies
10	Local sales representatives	Participant opinions on the importance of local sales representatives for cloud computing adoption
11	Market and sector knowledge	Participant opinions on the importance of knowledge of the German market and sectors for cloud computing adoption
12	Global surveillance disclosures	Impact of the global surveillance disclosures on the public cloud computing adoption of German companies
13	Economic espionage	Perceived risk of economic espionage through U.S. public cloud services
14	U.S. government reactions	Participant opinions on the reactions of the U.S. government to the global surveillance disclosures
15	German and EU government reactions	Participant opinions on the reactions of the German and EU government to the global surveillance disclosures

16	Data centre location	Importance of the location of the data centre for public cloud services adoption by German companies
17	Legal proceedings	Importance of legal proceedings by U.S. cloud providers for public cloud adoption by German companies
18	Cloud computing contracts	Importance of tailored cloud computing contracts for public cloud services adoption by German companies
19	Data encryption	Importance of the use of data encryption technologies for public cloud services adoption by German companies

This list of themes is the basis for the following phase, the production of the report.

4.5.6 Producing the report

The last phase involves the final analysis and write-up of the report. The purpose of this stage is to tell the "complicated story" of the data in a way which "convinces the reader of the merit and validity" of the analysis and provides a "concise, coherent, logical, non-repetitive and interesting account of the story the data tell" (Braun & Clarke, 2006, p. 93). Moreover, as maintained by Barbara Czarniawska (2003, p. 354), the objective is to produce a rich and thick description about the lived experiences of the respondents and that "generalization is not a job of an author, but of a reader". Consequently, the transfer of knowledge from one context to another requires that the reader understands both contexts (Wright & Ehnert, 2010). Nowell et al. (2017, p. 10) suggest that, at this stage, "researchers may consider how each theme fits into the overall story about the entire data set in relation to the research questions". Following this advice, the themes and findings are presented as listed in Table 22.

However, the discussion chapter is structured in relation to the objectives of the current research. Though, as with all qualitative studies, there is no hard boundary between the themes, and they can be related to more than one objective and be interconnected with each other. For example, the "Culture and history" and "Sector and size" themes also play a role in the "Salesperson trust" or "Foreign government trust" objectives. Table 23 gives an overview of the research objectives and the mapping of the themes for the discussion of the findings.

Table 23: Research objectives and themes

No.	Objective	Themes
1a	Importance of the concept of trust for cloud adoption	• Importance of trust
1b	Impact of the cultural differences	• Culture and history
1c	Influences of the sector	• Sector and size

2a	Product trust	• Cloud computing technology • U.S. cloud providers • Shadow IT
2b	Company trust	• U.S. cloud providers • German cloud providers • Private cloud
2c	Salesperson trust	• Local sales representatives • Market and sector knowledge
2d	Foreign government trust	• Global surveillance disclosures • Economic espionage • U.S. government • German and EU government
3	What U.S. cloud providers could do to improve trust	• Data centre location • Legal proceedings • Cloud computing contracts • Data encryption

To provide sufficient evidence of the themes, data extracts (e.g. quotes) need to be included to demonstrate the prevalence of the themes. N. King (2004, p. 268) recommends that short quotes should be used to “aid the understanding of specific point of interpretation” and more extensive passages of quotation should be included to give the reader “a flavour of the original text”. Following this advice, the presentation of the findings includes several quotes from buyers and sellers that should help to transport the individual voice of the respondents and the emotions and perceptions attached to their statements.

After the coding process I marked the sentences that I considered to be valuable quotes in the transcripts in Nvivo. Appendix 3: “Coding and notes writing” gives an example of a quote highlighted in green. Afterwards I translated these quotes into English to use them either in the findings and discussion chapters or to make them available as an additional reference in the appendix.

4.6 Role of the researcher

As described in Section 4.1, the research paradigm for the current study is constructivism. Wright and Ehnert (2010) advised that, when studying trusting, the task of the researcher is to produce an “authentic, engaging narrative that speaks of the lived experiences of actors” (Wright & Ehnert, 2010, p. 122). Hence, the authors cautioned against the temptation to make claims to generalization based on the constructed findings. This should allow scholars and practitioners to connect with the stories, relate their own experiences to them and learn from them (Wright & Ehnert,

2010). Put simply, “social constructionists should only ever claim to tell a partial story of trusting across cultures, not *the* story” (Wright & Ehnert, 2010, p. 124).

Furthermore, constructivists acknowledge the involvement of the researcher in the collection and analysis of data and recognise the subjectivity of their interpretations (Guba, 1990; Guba & Lincoln, 1994; Killam, 2013; Mertens, 2014). From the point of view of the constructivist researcher, “knowledge is constructed in process of social interchange” (Flick, von Kardoff, Steinke, & Jenner, 2004, p. 90) and “the researcher’s understanding is co-constructed with that of the participants through their mutual interaction within the research setting” (Given, 2008, p. 119). As maintained by Cunliffe (2003, p. 994), “research is as much about the world of the researcher (our experience, culture, language, and writing conventions) as it is about the world we are studying” and the researcher is constructing and making sense of social and organisational realities along with the research participants.

Constructivist researchers are constructing codes because they are actively naming data and because they choose the words that constitute their codes. Therefore, they need to engage in ongoing self-reflection and take their personal worldviews, assumptions and biases into account during data collection and data analysis. For the current research, I needed to be aware of the following two aspects regarding my cultural and professional background.

Firstly, I am employed by a U.S. cloud provider and my job involves selling U.S. cloud solutions to German companies. As stated above, my employer did not financially support my studies and did not have any influence on the research topic, design and results. In fact, I started my professional doctorate about one year before I worked for a U.S. company. To actively address this issue, all interview participants were informed about my job and the fact that my employer did not have any influence on the research design and results. These two influencing factors could, on the other hand, also be interpreted as a strength because of the unique access and insights that can be gained from this combination. My professional background and experience in cloud computing technologies and sales to German enterprise customers informed the aim and objective of the current research and were a valuable asset in the conversations with the interviewees. As described above, the constructivist paradigm holds the idea that the researcher and the participants are seen as co-creators of the

research findings. Consequently, it can be argued that my expert knowledge in this field had a beneficial impact on answering the research questions.

Secondly, I am a German citizen and share a cultural background with most of the interview respondents which might have an influence on the way I filter and interpret the respondents' statements. This also includes the translations between the English and the German language that were conducted by me which could also be biased by my own cultural background and my personal view on the matter. However, as described above, I did not translate the complete transcripts but only the quotes that I used in the findings and discussion chapters.

The concept of critical reflection in professional focus doctorates in not universally defined (K. Fisher, 2003; Reynolds, 1998; Sambrook & Stewart, 2008). It was, however, my aim to be fully transparent about my assumptions, values and beliefs as well as my social and professional background and potential biases that could have impacted the research findings. Therefore, critical reflection was a part of the entire writing process and is visible in several parts of the thesis.

In addition to these considerations regarding the role of the researcher, the following ethical aspects were taken into account.

4.7 Ethical considerations

Ethical matters need to be addressed "through all phases of the research study" (Creswell, 2007, p. 47) including getting access to research participants, gathering personal data and asking participants to give considerable time to the research interviews. This research was conducted under the guidelines of the "The University of Gloucestershire's Handbook of Research Ethics" which includes a statement of common ethical principles, procedures by which research shall be conducted and appendices addressing concerns in a variety of academic and professional fields.

The main concern of the research participants was the protection of the privacy and confidentiality of their names, the names of any other people or products mentioned in the interviews, and the names of their companies. Confidentiality is a fundamental ethical requirement of any research project (J. Harding, 2013). Particularly in business research, where the researcher often has access to sensitive organisational information, the researcher must ensure that potential ethical issues are addressed

appropriately (Greener, 2008). To proactively address this issue, a written agreement was offered to the participants of those organisations (see Appendix 2: “Participant recruitment”). This agreement stated that the names of the participants, products and organisations were anonymised and that the collected data was only used during this research. The agreement also affirmed that all audio recording and transcripts would be kept in a safe place where no other people had access to.

The close personal interaction with respondents requires that the researcher communicates his/her academic and professional position openly. As mentioned in Section 4.6, I conducted this research outside of and independent from my employer. However, since my employer is a U.S. cloud provider, it was important to inform the participants about the fact that this company did not have any influence on my research agenda and outcomes. To avoid any misunderstandings, all research participants were informed about my professional background before the interviews.

4.8 Summary

This chapter described the research design used for the current study. The chapter started with the selection of constructivism as the central research paradigm and went on to justify a qualitative research methodology to address the objectives of this research. The data collection was based on qualitative semi-structured interviews with 19 key informants from 10 German companies and 5 different U.S. cloud providers. The data was analysed using thematic analysis. This chapter also explained the role of the researcher and the ethical issues that were addressed in this study.

Having defined the research design, the next chapter presents the findings from the key informant interviews.

5 Findings

This chapter will present the findings of this study. As described in the research design chapter (see Table 22), a total number of nineteen themes have been defined and named, which will be presented in the following sections. Further quotes from the interviews can be found in Appendix 4: “Additional quotes”.

5.1 Importance of trust

Most of the buyers expressed that the concept of trust “played a great role” (Buyer04) in their decisions making process regarding public cloud computing adoption. In their opinion, it was just not feasible to exclude all possible risks and to protect themselves against dangers of all kinds. Therefore, they needed a business partner whom they could trust and who would take all necessary measures to ensure that their data and intellectual property was protected. As one of the key respondents pointed out:

> *„Yes, it is actually the deciding factor. If I wanted to try to make an IT system watertight to make sure that nobody can come in from the left or the right side, it is virtually impossible. We can set the hurdle or the bar as high as possible, but in the end, I have to find a partner whom I can trust. And this trust has been impaired by the American providers.” (Buyer03)*

Other key respondent highlighted the importance of trust for humankind in general and for all business transaction:

> *“So, I think that trust is important for every human being. Everything is based on trust. It will not work if I can’t build that trust, no matter what business model I have, no matter what.” (Buyer08)*

Several interviewees argued that trust needed time to develop and grow and required a long relationship. In their opinion, “trust needs to grow” (Buyer01) and it only takes a very brief time to lose trust, but it would take many years to rebuild it:

> *"Building trust in something like that is not a matter of individual actions but rather takes several years. One can break that with a single stroke, rebuilding it will take years." (Buyer06)*

The local sales representatives of the U.S. cloud providers made similar experiences with their customers. In their conversations with potential buyers, the topic of trust also played a vital role. They argued that cloud business was based on trust and that they would not sell cloud computing services through monetary incentives but by building trust relationships (e.g. Seller01). As highlighted by the cloud sellers, trust was important for IT services in general, but especially important for public cloud adoption:

> *"Trust is one of the most important concepts in any kind of IT service. This is especially true for public cloud services. Public cloud trust is especially important." (Seller08)*

According to the sellers, cloud was "a trust business" (Seller01). Consequently, the cloud sellers were actively aiming to build trust in their first meetings with their customers before they could start the conversation about technical product details:

> *"The topic is very important to me. The first two, three meetings are only geared to build trust." (Seller04)*

For several sellers, trust was the "most critical point in building business relationships" (Seller07) and it was "the biggest problem" (Seller05) if the IT departments of their customers would not trust them.

The buyers identified trust as a precondition for any business exchange. The sellers knew about this requirement and adapted their sales conversations to build a trustful relationship with their potential clients before engaging in any discussions regarding features or price. Overall, these results indicate that both the buyer and the seller see trust as a very important aspect in business relationships in general and in cloud computing services in particular.

Having presented the findings on the importance of trust, the following section addresses one of the core themes that emerged from the data, the impact of cultural differences between the U.S and Germany.

5.2 Cultural differences

A recurrent theme in the interviews was a sense amongst interviewees that one of the main reasons for the distrust of German companies in U.S. cloud services was a dissimilar cultural background between U.S. and German citizens.

The first aspect that was frequently mentioned by the respondents was the fact that Germany was known for having comparably strict data privacy laws and "an entire data protection culture" (Buyer02). As one of the respondents put it:

> *"There is indeed a reason why we have one of the most sophisticated data privacy laws. This doesn't happen by chance but evolves from the culture of Germany." (Buyer06)*

Some interviewees described that Germany was "very sensitive around these matters of privacy" (Buyer10) and had, in comparison to other countries, "very sophisticated" (Buyer11) data protection measures in place. They explained that everything in the country, including the data protection measures of the German government, was arranged to protect the personal information of the citizens (e.g. Buyer11). The key informants stated that "Germany demands a lot of transparency" (Buyer11) and that cautiousness was part of the German culture and independent from the NSA global surveillance activities revealed by Edward Snowden:

> *"There is a lot going on, and yet, we are in Germany, in my opinion, as usual, deliberately cautious. This has nothing to do with Mr Snowden." (Buyer09)*

The second aspect was about the history of Germany and its influence on the German culture. According to several respondents, an explanation for the different attitude towards government surveillance practices between the U.S. and Germany could lie in the history of Germany (e.g. Buyer08). The interviewees determined that the U.S. did not share the same experiences with national security agencies spying on their own citizens as Germany did in their history with the Nazi Secret State Police

(GeStaPo) and the State Security of the GDR (StaSi). They concluded that this was one of the reasons why the revealed practices of the U.S. intelligence agencies were not accepted in Germany. As one of the key informants explained:

> *"I believe that this is also a question of culture, starting with things such as a GeStaPo in the Third Reich or the StaSi in East Germany, where we already had such bugging operations and denunciation and eavesdropping operations. I think that, in consideration of those experiences, it is slightly more unpopular and unaccepted than it possibly is in the USA, where people didn't make those experiences to this extend in the past." (Buyer03)*

From the point of view of the buyers, one needed to take the history of a country into account to understand the cultural differences between the nations. They argued that the Germans would not understand the response of the U.S. to the 9/11 terror attacks and that U.S. citizens, on the other hand, would not understand the influence of the German history:

> *"I have to admit that I cannot understand why the American people responded to 9/11 the way they did. Conversely, the Americans do not understand our reactions to our SS-time. Because there are simply cultural differences." (Buyer01)*

Similar to the cloud buyers, several cloud sellers agreed that "history plays an important role" (Seller01) and that "Germans are especially sensitive of giving away personal information because of the Nazi and communism history" (Seller08). In their opinion, "a society which has been spied upon and which has been denounced over decades" (Seller06) was much more sensitive to data privacy matters. The fact that data was collected about many citizens by the government or even their neighbours over many years was not forgotten, especially by the older generations. One of the cloud sellers made the following comment:

> *"The past history is still a very big issue. It's not that long ago. The C-levels [CEO, CFO, CIO, etc.] have witnessed it themselves. The fact that files were*

collected about them has been etched on their memories. The knowledge that neighbours have collected information about me." (Seller02)

Furthermore, both groups, the buyers and the sellers, gave several examples to express their experience and views of the distinct cultural backgrounds of U.S. and German citizens. These examples suggest that the state played a different role in both countries which would explain some of the conflicts the buyers and sellers identified in the interviews. One example was that the German citizens would not understand why the U.S. did not have a public health insurance system and that the U.S. citizens on the other hand would not understand why the state needed to be involved in these matters or even called this a communism system:

"People in Germany cannot understand how one can be against a public health insurance system. And in America people are saying that such a welfare state has something to do with communism which they do not want. It's not their fault, this is culture." (Buyer01)

From their point of view, it could therefore be difficult for Germans to understand why U.S. citizens do not like the idea that the state gets involved in public health issues but that they accept that the government and private organisations collect and process personal information about them. Another interviewee argued that it was difficult for Germans to understand why the U.S. invested heavily into terror prevention but did not ban firearms for private citizens.

"It starts with the fact that when you know that in the USA every year 30,000 poor people die through the use of firearms and set this in relation to the 3,000 poor people who died because of the terror attacks on the 11th of September, one wonders: Why do the USA make such gigantic efforts to avoid one-tenth of the fatalities or to prevent it from happening again, whereas in their own country they fail to decrease or stop such stories or whatsoever." (Buyer03)

Other buyers commented on the willingness to share personal information and gave the example that people in the U.S. were very open with their salary whereas in Germany "you don't even really talk to your best friends about your salary" (Buyer02). As claimed by Buyer02, "American car dealers sometimes print their yearly salary on their business cards because they want to show how good they are". Likewise, Buyer03 argued that "in Germany one doesn't talk about certain topics like salary or these things. This is a cultural aspect". Others commented on the cultural difference in the willingness to use electronic payment methods (Buyer09) or argued that U.S. providers, because of the size of the U.S. domestic market, were not interested in geographical and cultural specifics. For example, Buyer10 stated that the U.S. "wouldn't know where Morocco is or New Zealand […] and therefore wouldn't think about as an impact on them". From the point of view of the buyers, U.S. citizens were used to constant surveillance practices and accepted the justification that this was for the safety of the country:

> *"I recently had a telephone conversation with a colleague from the USA who told me that only during his visit in Germany some months ago he realised what a huge topic this is. He said: 'As an American I'm used to the fact that the government is looking over my shoulder. Do I like it? No, but as long as I do nothing wrong, I do not have a problem with it.' The mentality of the U.S. citizens is obviously a bit different." (Buyer03)*

While the buyers commented primarily on the peculiarities of the U.S. society, the cloud sellers elaborated mostly on the distinctiveness of German citizens and companies. The local sales representatives of the U.S. cloud providers described the German people as "negative, cautious" (Seller03), "sceptical" and "conservative" (Seller01). One example was that Germans would even publicly protest against population census activities:

> *"Very high, I think. I believe that the topics around data protection and personal data rate high in Germany. Everyone is freaking out when there is a population census in Germany." (Seller05)*

The local sales representatives of the U.S. cloud providers explained that the discussions with their customers around the topic of personal data was in general very emotional and often subjective (e.g. Seller03). In addition, the cloud sellers argued that it was “more a gut feeling kind of argumentation by the customers” instead of a fact-based discussion (Seller08).

The sellers claimed that “Germans have a healthy suspicion about everything” (Seller06) and “want to understand everything bit by bit before they take the first step” (Seller07), whereas other countries would be more willing to take risks. For example, Seller06 commented that “while the American engineer is looking for innovations, the German is already looking for the downsides”. The cloud sellers further argued that German companies would not believe that the U.S. cloud solutions would be secure and that they had more trust in what they called German engineering.

Moreover, the cloud seller interviewees reported that other countries were more open regarding cloud technology adoption than Germany (e.g. Seller03; Seller04). In their experience, the Scandinavian countries and the UK were embracing cloud services, while Germany and Austria were more conservative with adopting cloud technologies:

> *“In my experience, in some EU countries, especially Scandinavia, UK and Ireland, the trust is from the start bigger and it is easier for U.S. cloud vendors.” (Seller08)*

Thus, several cloud sellers reported that “international companies have a different focus” (Seller07) and were more open and easier to convince than customers that were only present in Germany. From their experience, “the low-hanging fruits” were customers with an international focus (Seller03). They concluded that U.S. cloud providers would not try to please the special wishes and requirements of German companies if the population and buying power were smaller:

> *“If Germany wasn’t that big, U.S. cloud companies would not make such an effort to attend their special wishes.” (Seller05)*

Although the sellers mostly blamed the German companies for the slow adoption rate, they also acknowledged that the U.S. culture, on the other hand, would make it difficult

for German companies to build trust. They claimed that the U.S. would primarily focus on protecting itself against any external threats without taking the needs of other countries into account (e.g. Seller05). The respondents explained that the U.S. would think that if European countries had a problem with the decisions of the U.S. government, those countries had to find a solution to it themselves:

> *"This is again a cultural issue. We protect ourselves and if the Europeans don't like it, they need to do something about it themselves." (Seller04)*

The buyers concluded that the cultural difference between the U.S. and Germany was also the reason why there would not be any substantial changes to the U.S. law anytime soon (e.g. Buyer02). Although they acknowledged that cloud computing was disrupting current business models, they argued that it was difficult to change a culture that developed over hundreds of years:

> *"I mean it is hard to undo 500 years, 800 years of culture. Yes, the Internet is a disrupter, yes cloud can be a disrupter, but I'm not going to undo 500 or 800 years." (Buyer11)*

However, both buyers and sellers recognised that younger people were already "more open" (Seller03) regarding modern technologies including public cloud services. They stated that "companies with younger employees are much easier" and that "the younger people rather see the opportunities" (Seller03) instead of the risks. As one of the buyers explained, this was "probably also a generational issue" (Buyer07):

> *"So, my 19-year-old daughter has a completely different relationship to data and willingness to share data than basically… yes, let's say my generation, where you still consider carefully if you provide certain data, if you share them, that's what I think." (Buyer07)*

According to the sellers, this was also the case with younger CIOs and IT managers who would "have a different view" (Seller06) on cloud services and data privacy matters than their older colleagues.

Taken together, the buyers and sellers agreed that the U.S. and Germany showed several cultural differences and that these cultural distinctions could have an impact on the purchase decisions of German companies regarding U.S. cloud services. The cultural characteristics of these two groups will be analysed in more detail in the discussion chapter. Another prominent theme that emerged from the data which will be discussed in the following section was the influence of the sector and size of a company on the stance towards U.S. cloud services.

5.3 Sector

One assumption of this thesis was that there was no considerable difference in the cloud computing adoption between sectors (or industries) in Germany (see Section 2.1.5). The findings suggest, however, that some sectors are more open to public cloud services whereas others are rather reluctant to migrating their data to public cloud providers.

A prominent example were insurance companies. A few participants explained that the German insurance industry had certain regulatory restrictions regarding cloud computing (e.g. Buyer07). Buyer01 stated that “German insurance companies are subject to relatively high regulatory and legislative requirements”. According to the respondents, this made it “almost impossible” for insurance companies to use public cloud services (e.g. Buyer01). However, there were also certain sectors or industries which had less reservations about the use of public cloud services. As stated by Buyer02, “it always depends very much on the industry”.

From the point of view of a few interviewees, the risk for some businesses (e.g. media companies) for using cloud computing services was comparably low in relation to other industries:

> *“If we have a data breach, while it may be serious that there is a data breach, the consequences of that are less than perhaps other types of data breaches or other types of businesses.” (Buyer10)*

They argued that even if a data breach was not without any impact on their business, it would not be “a danger for life and limb” (Buyer10). Therefore, the strategies regarding external data processing and sharing were very different from company to

company and depended on the companies' business models. One interviewee explained that some companies only had a corporate website online while others would run business critical applications in the cloud (Buyer09).

The local sales representatives of the U.S. cloud providers agreed with the key informants of the German companies on the fact that the sector or industry a company was operating in had a considerable influence on the adoption of public cloud solutions from U.S. providers.

In addition to the sector or industry of a business, the size of the company was also seen as a factor influencing the cloud provider decision. From the perspective of several respondents, larger corporations were in general more open to adopting public cloud solutions. This was particularly the case where they operated globally and if the German law did not make it difficult for them to store their data in public cloud data centres. As one of the sellers explained:

> *"The size of a company has an influence on cloud adoption, especially if they are international." (Seller07)*

Another explanation mentioned by the key informants was that larger companies had more buying power and thus more influence on the contracts with U.S. cloud providers and could also make suggestions for future product developments:

> *"In comparison with the really big companies it is very difficult for us. It is extremely difficult for us to influence anything, that's the way it is" (Buyer09)*

Medium-sized businesses in Germany were, however, from their experience, not very open to cloud services. As one of the cloud sellers argued:

> *"A classic medium-sized company, industrial companies, will not be very open-minded, doesn't want to learn." (Seller01)*

In contrast, start-up companies were considerably more open to exploring the possibilities of cloud computing and, according to the sellers, some of them "couldn't do their business without the public cloud" (Seller08). The cloud sellers noted that start-up companies could not afford to lose business if the performance of their

software applications was not sufficient and would therefore host their data and applications at large U.S. providers (e.g. Seller08). The impact of the sector a company is operating in on topics such as cloud adoption, legal constraints, shadow IT, economic espionage and the trust in local salespeople will be discussed in more detail in the next chapter.

The following section will focus on the view of German IT decision makers on the advantages and downsides of public cloud computing technologies.

5.4 Cloud computing technology

Most of the respondents did not have any reservations to the cloud technology itself and acknowledged the technological benefits of cloud services as described in the background chapter. Whilst a minority mentioned that the term cloud was sometimes saddled with negative associations (e.g. Buyer07), almost all agreed that cloud computing was the next logical step in the evolution of IT and an irreversible process. The respondents had no doubt that cloud services would provide the reliability and performance required by their businesses (e.g. Buyer08). It was therefore no option for them to remain passive and ignore the developments in the IT industry (e.g. Buyer03). Some respondents even describe themselves as staunch supporters of the cloud computing concept. For example, Buyer01 said that he was “an advocate of the cloud” and that there was “no way around the cloud”.

As one might expect, the cloud sellers had “no doubt that the future will be in the cloud” (Seller07). They reported that most of their customers would share this view about cloud computing technologies and that “nobody is doubting” the “technological capabilities” (Seller06) of large cloud providers anymore. As one of the cloud sellers stated, “the product is never the problem” and “trust in the product is usually existing (Seller05).

From the point of view of the German companies, key drivers for public cloud computing adoption included flexibility, shorter time to market, cost savings and other benefits of using cloud computing (e.g. Buyer03; Buyer05). For some of the interviewees, cloud computing made most sense in a SaaS delivery model (see Section 2.1.2). They explained that one of the major drivers was that the software in the cloud would always be up to date and that they would “get a solution in the cloud

and not only cloud space" (Buyer08). For other participants, the key benefits of cloud computing solutions were especially in customer focused (B2C) or in business partner (B2B) scenarios:

> *"So how we exchange data with our customers. This could be done very well with a cloud." (Buyer06)*

According to their explanation, this included secure email communication, document sharing and mobile applications.

This view was also shared by the cloud sellers. From their experience, most of their German customers would acknowledge the fact that cloud providers can run IT services more efficiently than they could in their own data centres, especially in terms of elasticity and agility (e.g. Seller05). For example, Seller06 argued that "today, most customers acknowledge the fact that the renowned cloud providers can run IT better than they could do it themselves". All in all, they estimated that cloud computing had an immense potential in Germany which was currently unexploited (e.g. Seller04). However, they admitted that it was not always clear to German companies how to leverage the features of cloud technologies for their business (e.g. Seller07).

Notwithstanding the trust in the cloud computing technology, the German companies required a provider that they could trust with their data and who could guarantee that no company secrets were given to their competitors in the U.S. or other countries. As explained by one of the key respondents:

> *"This [cloud computing] makes perfect sense, I just need partners whom I can trust and where I can be sure that my data doesn't end up in the hands of our U.S. competitors." (Buyer03)*

To mitigate their risks, they were looking for cloud solutions that met their security requirements and were certified for their line of business (e.g. Buyer09; Buyer11).

In summary, these results show that both buyers and sellers experienced that German companies acknowledge the potential business benefits of cloud computing technologies. The discussion chapter will examine the potential contradiction between the potential cloud benefits and slow cloud adoption. Since the cloud computing

technology was probably not a reason why the cloud adoption of German companies was comparatively low, the next section will look into the opinions of the respondents regarding the features and maturity of U.S. cloud services.

5.5 U.S. cloud services, features and maturity

A common view amongst the interviewees was that the features and maturity of the cloud services of U.S. providers were in general superior to the cloud offerings of German or European cloud providers. They explained that "there are no solutions form German companies that can compare to solutions from companies such as Microsoft" (Buyer03) and that most of the recent developments in technology were only available in Europe at a later point in time. For example, Buyer11 reported that "the majority of the most important cloud software providers tent to come from North America". In their opinion, certain technologies may even never be available from German or European cloud providers. As one key respondent argued:

> *"Most major global players just don't come from Germany or Europe. How do you want to create a cloud solution like those from Microsoft or Amazon in Germany or Europe?" (Buyer01)*

Furthermore, Buyer01 claimed that "the American provider may be 2, 3, 4 years ahead of the German cloud solutions". Likewise, Buyer05 commented that he could not "think of any alternative which is as comprehensive" as the products of the U.S. cloud providers.

The local sales representatives of the U.S. cloud providers shared the view that U.S. companies were driving the general global cloud development and were superior to cloud services from Germany or other countries in Europe (e.g. Seller04; Seller05; Seller06; Seller07; Seller08). From their experience, their German customer knew about this situation:

> *"They see that the U.S. companies are the market leaders and if you want to do serious cloud computing today you have to use the U.S. cloud services. Only these companies give you the speed of development and speed of innovation." (Seller08)*

They explained that cloud infrastructure investments were very cost-intensive and that only a few companies could afford that. Consequently, the cloud sellers identified other U.S. companies as their main competitors on the German market and not companies from Germany or Europe. As stated by one of the cloud sellers:

> *"Our competitors only come from America. Individual niche players come from Germany and are rather less present." (Seller04)*

Several key respondents of the German companies explained that there was no viable alternative to the cloud solutions of the U.S. cloud providers, especially in the field of office productivity solutions. The respondents had looked at alternative products from German and European companies, but they did not meet their demands in terms of standardised software interfaces and the integration with popular smartphone and tablet apps (e.g. Buyer05; Buyer06; Buyer08; Buyer11). For example, Buyer08 believed that "this doesn't exist in Germany". In their opinion, Asia was much more likely to compete against U.S. cloud providers than Europe or Germany in the future (e.g. Buyer11). Another key differentiator between cloud offerings from U.S. cloud providers and European or German providers was the price (e.g. Buyer02).

The cloud sellers agreed with the buyers on the capabilities of German providers and added that most cloud offerings in Germany were either no real cloud services or they were using U.S. software products but with limited functionalities (e.g. Seller06; Seller07). They stated that many European cloud providers were only classic server hosting companies "re-labelled in cloud hoster or cloud provider" (Seller01). They also claimed that most of the European providers could not automatically upscale their infrastructure (e.g. Seller01; Seller08) which is, however, a key condition of a cloud infrastructure (see Section 2.1). For example, Seller06 commented that "the great cloud breakthrough is just not coming from Germany. Germany is not sufficiently active but has rather the foot on the brake".

Some interviewees from the German companies tried to find an explanation for the disequilibrium between U.S. and European cloud offerings. One of those explanations was that the U.S. companies started much earlier with the development of public cloud solutions and that the size and business potential of their own domestic market gave them a competitive advantage over many other countries (e.g. Buyer03). Another

explanation was that there were not many IT and software development companies in Europe or Germany and that this was therefore also the case for cloud computing solutions (e.g. Buyer11).

In summary, most of the key informants of the German companies and the local sales representatives of the U.S. cloud providers rated the U.S. cloud services as superior to German cloud solutions. The conflict between the trust in U.S. cloud providers, the capabilities of German/European cloud providers and popularity of the local data centres of the German companies will be analysed in more detail in the discussion chapter. Another theme that is closely linked to the features and maturity of U.S. cloud services is the distribution of public cloud shadow IT services within German companies. The following section will report the findings regarding shadow IT from the perspectives of buyers and sellers.

5.6 Shadow IT

From the experience of many of the buyers, there was a push of consumer technologies into the business IT and organisations which suddenly had to deal with topics such as “bring your own device” (BYOD) and corresponding cloud services. They explained that, in the past, the IT departments decided what devices and software should be used by the employees. However, nowadays the employees demanded devices and services that they were used to work with at home and when they were on the road. As explained by one of the buyers:

> *“Well, in the past we set the technology standards, we provided them, from the corporate point of view. Now it is more coming from the consumer, from what I use at home.” (Buyer07)*

Several of these companies offered their employees official and secure IT solutions but they were also aware that some of their employees might use a separate way to store and exchange company data (e.g. Buyer09).

Most companies had strict policies prohibiting the use of external online services. However, several respondents admitted that employees might be using consumer cloud services like real-time communication and file sharing applications for their professional work which were not approved by the IT departments and were not

compliant with their IT policies (e.g. Buyer02). For example, Buyer07 admitted that he assumed that “this is done”.

The cloud sellers affirmed that German companies had an issue with shadow IT. From their experience, cloud software was often introduced to companies by their employees without the knowledge of the IT departments. They explained that employees would bring their own devices including their own software and cloud services to fill the gaps that their companies’ IT departments could not provide. As one of the cloud sellers reported:

> *“But then they are using Dropbox or something similar. Shadow IT is in these cases always in the cloud.” (Seller05)*

Some of the sales representatives of the U.S. cloud providers claimed that it was often the senior management of those companies who were using non-compliant services themselves (e.g. Seller07). From their point of view, the senior management should act as a role model by using secure devices and software. Nevertheless, while most traditional businesses tried to stop shadow IT to avoid data leakages, a few companies, e.g. in the media industry, embraced the diversity and flexibility of shadow IT (e.g. Seller08).

The key respondents of the German companies argued that there was no way to entirely prevent any use of unauthorised IT services (e.g. Buyer08). As reported by one of the IT managers of the German companies:

> *“You cannot prevent this. Officially this doesn’t exist here, it is also not offered as a product and should not be used.” (Buyer05)*

The IT managers stated that they could not monitor all user activities and could therefore not prevent their employees from using IT services that were not company standard (e.g. Buyer09). In their experience, it was not possible to prevent shadow IT with monitoring tools but only by meeting the business needs of their employees together with corresponding training initiatives (e.g. Buyer08).

The cloud sellers assessed the existence of shadow IT as a security risk for the German companies. For example, Seller07 warned that shadow IT was “always there

in every company" and that shadow IT was "a huge risk". From his perspective, the risk that company employees are secretly using unauthorised cloud services might be higher than the risk of companies migrating their business data to the cloud.

However, on the other hand, the existence of cloud-based shadow IT at German companies could be used as a sales tactic by the sellers. One of the cloud sellers explained:

> *"This is also a good approach to sell that: You are surely using cloud, you just didn't know about it yet." (Seller05)*

Nevertheless, the sellers made the experience that their customers did not want to talk about the probability and risks of shadow IT with them. From the point of view of their customers, shadow IT was an internal matter which needed to be discussed internally (e.g. Seller07).

Together these findings provide important insights into the distribution of shadow IT cloud services in German companies. Despite the known risks of shadow IT services and even if the use of this software was officially prohibited by company directives, employees of German firms were actively using cloud-based software such as file sharing and instant messaging. This finding suggested that a lack of interest in or need of cloud services was no reason for a low cloud adoption by German companies. The discussion chapter will debate the lack of alignment between business and IT departments with regards to public cloud service usage in more detail.

5.7 U.S. cloud providers

Most of the respondents of the German companies did not believe that the U.S. cloud providers had a vested interest in proactively providing U.S. intelligence agencies with customer data but rather assumed that the U.S. companies would only act under the pressure of the U.S. law enforcement. For example, Buyer03 argued that the U.S. companies were "smart enough to know that this can only have a negative impact on their business" and that they were "not doing this voluntarily but under constraint". They reasoned that, if U.S. technology companies wanted to collect private company data, firms such as Microsoft could have built backdoors in their computer software a

long time ago and would therefore also have access to the data stored in the on-premise data centres of German companies (e.g. Buyer05; Buyer08).

The respondents argued that the U.S. cloud providers and the U.S. government had very different motives. While the U.S. cloud providers would want to grow their businesses, the U.S. government agencies were interested in collecting as much data as possible (e.g. Buyer11). From their perspective, the U.S. cloud providers were themselves interested in solving this conflict and would put their own business model at risk if they cooperated with the U.S. intelligence agencies by providing customer data to them (e.g. Buyer07).

Likewise, the cloud sellers did not believe that their employers were actively involved in the NSA surveillance activities (e.g. Seller05). In their opinion, the U.S. cloud providers were interested in a relationship with their customers that was based on trust. For example, Seller05 believed “that American companies are very afraid of losing public trust”. They told their customers that the U.S. cloud providers were also upset about the NSA surveillance activities and that there were no backdoors implemented into their software (e.g. Seller06). Moreover, the cloud sellers defended their employers by saying that the U.S. cloud providers, as any other company, had to comply with the law (e.g. Seller07). They claimed that their customers would understand that terror prevention required certain actions by the U.S. government and the U.S. cloud providers (e.g. Seller08).

Nevertheless, since the U.S. companies were subject to the U.S. legal system, they did not have a choice but to cooperate with the U.S. government bodies (e.g. Buyer05). The key informants of the German companies therefore assumed that there was no way the cloud providers could defend themselves against the practices of the intelligence agencies (e.g. Buyer01; Buyer03; Buyer04) and were therefore avoiding U.S. cloud providers (e.g. Buyer04). As commented by Buyer01, “the American cloud providers can do little if the American government is not doing anything. They are subject to the underlying legislations which they cannot shake off”.

Furthermore, they stated that because the National Security Letters would not allow the corporate leaders of the U.S. cloud providers to speak about their cooperation with the U.S. government (see Section 2.2.1) they would not know if they were lying to them (e.g. Buyer04). As one of the buyers explained:

> *"I cannot even trust the statements of the chief executives of those companies since they are partly obliged by law to lie. This is because of the national security letters." (Buyer03)*

For these reasons, the German companies decided that the risk of using U.S. cloud services outweighed the benefits of the technology provided by the U.S. companies. As one of the IT managers stated:

> *"The risks of using these providers and services are basically higher than the opportunities and benefits to become more competitive." (Buyer07)*

They clearly preferred a German or European cloud provider because they did not like the idea that the U.S. government could get access to their company's data (e.g. Buyer04). In their opinion, U.S. cloud providers "cannot do anything substantial" (Buyer07) to rebuild the trust of the German companies.

The local sales representatives of the U.S. cloud providers echoed the view of the buyers that many German companies were afraid of the fact that the NSA could access their data. They explained that a large majority of German companies were aware of the NSA surveillance activities and would prefer to keep their data in Germany (e.g. Seller06). In general, customers were more sensitised since the Snowden revelations and more cautious about using U.S. cloud services. The cloud sellers acknowledged that they could not promise that the U.S. government would not find a way to get access to customer data stored in data centres managed by U.S. cloud providers. For example, Seller05 admitted that he could not "guarantee that no NSA employee has access to the data".

They further explained that data encryption using encryption keys provided by the cloud consumer would be the only way to guarantee that the U.S. government would not get access to the data. As long as there was a way for the U.S. cloud providers to access the data, they would have to do it when the U.S. government required them to give it to them and when it was compliant with U.S. law (e.g. Seller07).

All in all, the German companies trusted the U.S. cloud providers more than the U.S. government (e.g. Buyer11). The cloud sellers came to the same conclusion that their

(potential) cloud customers had more trust in the U.S. cloud providers than in the U.S. government, while some providers were regarded as more trustful than others (e.g. Seller08). As one of the cloud sellers explained:

> *"It's not so much the U.S. companies but more the U.S. government. They trust U.S. cloud providers, but they don't trust the U.S. government."*
>
> *(Seller07)*

However, the scepticism of a few respondents was not only against U.S. cloud products but also against U.S. technology products in general. They criticized that "American technology is built in everywhere" (Buyer03) and that there was technology from U.S. companies such as Apple, Cisco, Dell, HP and IBM in great parts of their IT infrastructure. They explained that if the NSA was not spying on them at the higher levels of the ISO/OSI model, they could also do it anywhere in between (e.g. Buyer03). Consequently, they would prefer to "replace all sorts of U.S. products" with products from German or European companies (Buyer04).

The following section will focus on the public cloud providers in Europe and Germany and their responses to the global surveillance disclosures.

5.8 German cloud providers

Several key respondents expressed that German IT companies would take advantage of the current uncertainties regarding the potential access of U.S. intelligence agencies to customer data and that they would use this momentum themselves if they were a German cloud service provider. As stated by one of the key respondents:

> *"If I was a German medium-sized business I would really play the card and try to develop offers to alienate customers from the American companies."*
>
> *(Buyer03)*

The cloud sellers agreed that the German IT industry took advantage of the NSA surveillance scandal and actively advertised cloud services "Made in Germany" (e.g. Seller04; Seller05; Seller06). They acknowledged that they probably would have had a higher cloud revenue in Germany without the NSA surveillance scandal. For example, Seller05 commented that U.S. cloud providers for sure "had more revenue

if the NSA issue did not exist". From the point of view of the sales representatives, the "Made in Germany" tag was the only advantage the German cloud providers had over the services provided by U.S. cloud companies (e.g. Seller07). They maintained that the arguments presented by German cloud providers for hosting data with them was merely a sales strategy and did not have any legal imperative. As one of the sellers argued:

> *"Many German cloud providers are now responding to this. This is not a legal topic but a psychological topic." (Seller06)*

Additionally, the cloud sellers claimed that many German companies that called themselves cloud providers were actually only IT outsourcing and IT hosting companies that used the term cloud as a marketing vehicle but would not truly offer the technological benefits of a public cloud provider (see Section 2.1.3) such as rapid elasticity (e.g. Seller08). As explained by another seller:

> *"There were German cloud providers and outsourcers and hosters, that call themselves cloud providers, in my experience with not so much success. While they have advantages on the legal aspects, they are missing most of the features that you can get from the big U.S. providers." (Seller08)*

Nevertheless, even if the data was not actually more secure with a German cloud provider (e.g. Buyer05), the trust in German companies was higher than in U.S. providers and the trust in German products was "much higher than in the average of European products" (Buyer04). As an example, a few key respondents of the German companies reported that their own customers, as well as the customers of their customers, required that all data was stored in Germany. Some of their clients insisted on written agreements that they were not storing or processing any of their data outside of the EU or even outside of Germany. These interviewees claimed that this requirement was not because of legal requirements but mainly driven by fear and that their customers were afraid of getting involved in any kind of data privacy scandal (e.g. Buyer02). However, these German companies and their customers could also use this restriction as a feature and actively advertise the fact that they did not store any data with an U.S. cloud provider. As explained by one of the buyers:

> *"Firstly, it is a requirement from the customer to us. And secondly, by transforming this requirement into a feature, we can differentiate ourselves from the competition." (Buyer02)*

These findings suggest that both buyers and sellers noticed that German cloud providers tried to take advantage of the global surveillance scandal but could not compete on the technological level. This aspect will be examined in more detail in the discussion chapter.

Another alternative to public cloud providers is the on-premise data centre of the companies and the operation of a private cloud which will addressed in the following section.

5.9 Private cloud

Notwithstanding the trust in the cloud computing technology itself (see Section 5.4) the advantages of a public cloud deployment model (see Section 2.1.3) and the efforts of German cloud providers (see Section 5.8), most of the key respondents of the German companies preferred to implement their own private cloud solution instead of migrating their data to public cloud services. As one of the buyers stated:

> *"But the goal will always be that we are not using the cloud service but that we are basically buying the whole package and hosting it ourselves. So, the cloud would be provided by [Company06] in our own data centre." (Buyer06)*

The interviewees gave a couple of reasons why they preferred their own data centres over public cloud solutions. The most frequently cited reasons were the global surveillance disclosures and general security and data privacy concerns. Some respondents categorically ruled out the storage of certain data (e.g. personal data, payroll, etc.) in a public cloud infrastructure (e.g. Buyer06; Buyer09). For example, Buyer06 explained that there was "no reasonable security solution for the cloud" and that the public cloud was "an uncontrolled space" and "a legal vacuum". Likewise, Buyer05 stated that "there are departments which are that strategic or important" that his company would not "even accept the slightest risk that someone looks in there". They argued that they could only move, if any, commodity workloads such as social

blogging tools to the cloud. Core business applications and mission critical workloads, on the other hand, needed to stay on-premise in a private cloud infrastructure (e.g. Buyer11). Even companies that were already using U.S. cloud services were still not convinced that they could trust the cloud providers with all their data. They acknowledged that there was a remaining risk that their data could get into the wrong hands and they therefore excluded several departments such as research and development from their cloud strategy (e.g. Buyer05). They furthermore claimed that their company would only know if they were hacked and what business was impacted when the systems were in their own data centre and not with a public cloud provider (e.g. Buyer11).

The sellers confirmed that "the trust in the local data centre provider is still high in Germany" (Seller06). They explained that their customers would have the opinion that their data would be safer in their local data centres than in public cloud environments. However, the local sales representatives of the U.S. cloud providers argued that most data leaks came from inside an organisation and that cloud data centres provided better security than the local data centres of their customers:

> *"When it comes to data security and privacy of data, companies tend to have a significantly higher trust in their own IT organisation than in any external vendor. This is in my view not valid since most data leaks come from inside and not from outside." (Seller08)*

From the point of view of the cloud seller respondents, the weakest point in IT security was usually human involvement. They claimed that the highly automated processes in the cloud data centres had superior security compared to the manually administered on-premise servers of their customers. The cloud sellers reported that when they got the chance to explain the public cloud benefits to their customers, they would understand that cloud data centres meet higher security standards (e.g. Seller07) and provide greater agility and scalability (e.g. Seller08) than their own facilities. For example, Seller07 claimed that "if you talk about access with the customer, they understand that they cannot compete with cloud security". Moreover, as argued by Seller08, most data leaks would come from inside an organisation and not from outside.

The second most frequently mentioned rationale was about personnel-related matters. A few key respondents expressed the opinion that they had more trust in their own staff than in an external cloud service. For example, Buyer10 argued that he did not "necessarily distrust the cloud", but that he had trust in his current provider "to a great degree" and that a new cloud provider therefore had "to overcome that". He further explained that this current provider would know his business very well and that he would therefore be "very trustful of that relationship". In their experience, their own IT data centre managers understood their companies' businesses and needs and were therefore able to provide a better service than any external provider. From their point of view, it was not a matter of cloud distrust but about trusting their own organisation more. Another aspect was that some companies were afraid of losing technical skills and competencies if they would move their IT to the cloud. For example, Buyer08 argued that by outsourcing his IT he would thereby lose some of his "in-house competencies". In contrast, the local sales representatives of the U.S. cloud providers argued that German companies and especially SMEs were not able to provide IT services with the same level of quality and security as the services provided by the U.S. cloud providers.

Moreover, the sellers claimed that German companies were too proud of their own IT competencies and would think that they could provide services that were as good or better than U.S. cloud services. As argued by one of the cloud sellers:

> *"I believe that this is also a matter of pride for the Germans. Germans are unwilling to acknowledge that Americans are better in something. At the back of their minds, Germans believe that they can do it better themselves."*
>
> *(Seller06)*

The third argument that the German companies presented was that they did not believe that they would save any costs when moving to a public cloud service. They argued that they could achieve similar efficiencies and cost structures in their own data centres and that cloud storage capacities were not an incentive to move to the cloud. For example, Buyer10 explained that "people talk a lot about it saving cost" but he "hasn't really seen it" because his company had "pretty good scale" in their own data centres. Likewise, Buyer08 commented that modern servers would require less space

and energy than they needed 10 years ago and that “this cannot be a cost factor anymore”.

Taken together, these findings suggest that the buyers believed that they would be better off building their own private cloud in their local data centre. The sellers confirmed this trend among German companies but argued that these self-constructed solutions would not be able to compete with the features, performance and security of U.S. cloud services. The potential contradiction between the advantages of public cloud services and the preference of German companies for on-premise solutions will be addressed in the discussion chapter.

5.10 Local sales representatives

Most of the cloud buyer respondents stated that the relationship to their local salesperson was not of much importance for them. They argued that they were primarily interested in the product itself and that the salesperson would not change their opinion about it. For example, Buyer05 said that “some are nice, they are all salespeople, but I don’t think that this had anything to do why we chose them.” He added that if the salesperson “would have been completely unsympathetic” he “might have kicked him out eventually”. Another interviewee gave the following example:

> *“If you want to buy a car and you don’t like the seller then you go to a different showroom. But the car remains the same anyway. I had a close look at it before I knew the seller.” (Buyer06)*

The IT managers preferred to compare different IT solutions themselves before even contacting the company or salesperson. From their point of view, it was more important that they could rely on the entire organisation of their business partner rather than on a few salespeople (e.g. Buyer10). In addition, as explained by Buyer09, “what the technology can really do is often not what the salesperson promises”.

One of the arguments by the German companies was that they believed that the local sales representatives of U.S. cloud providers in Germany had not enough power to make important decisions and had no substantial impact on the design and configuration of the cloud products. In their opinion, the cloud sellers were not being provided with relevant information about any cooperation of their companies with U.S.

law enforcement agencies and were therefore not in the position to make any promises or give any guarantees. As one of the buyers commented:

> *"Even if they were the most reputable and most honest citizens I could think of, none of them can guarantee anything." (Buyer04)*

Likewise, Buyer03 claimed that he knew "how these people are fed with information" and that they were "in no way involved in these matters in the background". Buyer03 also reported that salespeople were "desperate to find arguments to defuse the threat situation" but that he did not hear a single argument that would convince him. Additionally, they argued that American companies were "traditionally highly centralised and controlled from the USA" and that the cloud sellers needed to ask their headquarters in the U.S. for approval, even for minor issues (e.g. Buyer03; Buyer11). The buyers therefore preferred "to talk to somebody in the home organisation" (Buyer11) instead.

In contrast to the buyers, the cloud seller respondents argued that it was important to have local sales representatives in Germany. According to the cloud sellers, German companies wanted to have German contact persons that speak German and it was a competitive advantage for foreign companies to have local salespeople that could visit potential customers (e.g. Seller01; Seller05; Seller06). As one of the cloud sellers described:

> *"The companies want German contact persons. Also, a big German branch office with German service, with a main contact, a salesperson contact." (Seller05)*

In the experience of the cloud sellers, German customers would want to see the face of the person they were doing business with. As stated by Seller02, "nothing happens here without the first handshake". Another seller explained that it was "definitely a competitive advantage when there is somebody in the field, when the people have a face" (Seller06). Especially in the cloud planning process it was important for the customers to have a dedicated contact person (e.g. Seller04; Seller07). They argued that "a personal conversation is particularly important to understand the biggest pain in the company" (Seller03) and that especially "larger companies prefer a personal

contact who they can talk to" (Seller04). Likewise, Seller08 maintained that "enterprise customers would not buy U.S. cloud services without a local sales representative".

The cloud sellers, as opposed to the buyers, claimed that it did not work to sell U.S. cloud services centrally from the USA to the rest of the world or from a call centre in Europe. They further explained that their inside sales teams would not be able to replace their field salesforce and that their field sales employees were the face of the company (e.g. Seller03). And without a field sales team their customers would not get any onsite presentations, demos, or workshops. From their experience, personal conversations were vital to establish a basic trust level and to get into an advisory role (e.g. Seller03). For example, Seller04 maintained that "trust in the salesperson is even more important when it is about a real cloud plan". Additionally, the sellers described that "it helps enormously if you speak German" (Seller05) and they would not hire any field staff without German language skills. For example, Seller06 maintained that he has "not hired anybody yet who did not speak German".

Taken together, buyers and sellers had divergent views on the importance of local sales representatives for the adoption of public cloud services by German companies. Whereas the buyers claimed that they would not require the help of a local salesperson, the sellers reported that their clients would ask for German-speaking local resources. These differing perspectives are discussed more thoroughly in the discussion chapter.

Another aspect of the trust in the local sales representative might be their expertise in the market and sector of their potential customer. This theme will be addressed in the following section.

5.11 Market and sector knowledge

Several respondents stated that their business partner needed to have a certain level of sector knowledge and have a general understanding for the German market (e.g. Buyer08). As stated by one of the key informants:

> *"So, you need someone at the cloud provider who knows the national circumstances and sector-specific characteristics inside out." (Buyer01)*

Likewise, Buyer10 explained that “you need to have some context” about what the customer is doing to provide the best solution. The IT managers of the German companies argued that it would take a long time to explain the German legal constraints and regulations as well as the business needs of German companies to a U.S. company. They expected their business partners to have the same way of thinking, mind-set, and reactive spirit as their own employees (e.g. Buyer10). From their perspective, it was the responsibility of the cloud provider company to employ reliable, competent, and committed people. They argued that the employees mirrored the philosophy and culture of the company they worked for and that companies could influence this through “recruitment, personnel selection, personnel qualification” (Buyer07) and other measures. Though, not all buyers believed that the sales representatives of the U.S. cloud providers would have the necessary expertise to give the best advice to their German customers. For instance, Buyer08 said that he would not trust “an Amazon employee” that he or she understands his business and takes care of him”.

The local sales representatives of the U.S. cloud providers agreed that, in order to be successful on the German market, it was important for them to know the specifics of German companies and industries. As contended by Seller08, “it is not only helpful, but it is actually required to have industry knowledge”. They argued that it was important for them to be able to speak the jargon of their target sector and to know the technical vocabulary and business practices. One of the cloud sellers explained:

> *“If I’m going to a machine builder and to a media agency on the same day, they will need completely different solutions. The language of the respective industry is very important. If you don’t speak it, it may backfire.” (Seller05)*

The sales representatives argued that customer references would be more convincing to German companies than any product features or promises made by salespeople. For example, Seller08 said that “the biggest trust customers have is in other peers in other companies”. As soon as they see that their peers have trust they are ready to trust cloud providers. Success stories help significantly, get customers together and talk about their experiences, etc”. As another seller summarised:

“It is important to have references in the sector or industry to convince the customer.” (Seller07)

In summary, both buyers and sellers agreed that knowledge of the German market as well as of the sector or industry was important for selling cloud services to German companies. However, not all buyers were convinced that the local sales representatives of the U.S. cloud providers would have this knowledge. The discussion chapter will examine the importance of local sales representatives and the necessary market knowledge in more detail.

5.12 Global surveillance disclosures

Most of the key respondents stated that the Snowden revelations had caused great uncertainty and raised many concerns among German enterprises. Both the intensity and extent of the revelations were a shock for the German companies (e.g. Buyer06). They reported that the NSA surveillance activities were the biggest scandal of the last years and led to a significant loss of trust. As commented by one of the interviewees:

“I must honestly say that what has been revealed in the last 1-2 years by the Snowden publications is an extreme breach of trust.” (Buyer03)

Several interviewees stated that the revelations of Edward Snowden exceeded their worst suspicions and that thoughts that they considered paranoia before turned out to be real. Additionally, they argued that the possibilities of backdoors in products of U.S. technology companies was discussed for many years and that they now had proof that those existed. For example, Buyer04 stated that he was not “in the position to tell if the outcry of these companies in the press is just practiced marketing”. Furthermore, Buyer07 commented that he heard that “there has actually been some cooperation between companies such as Apple and Google with relevant institutions, state bodies” and that this was in his “view a new quality where they ultimately set their own business model at stake”. Similarly, Buyer03 concluded that at “this point, you can only try to protect your data as effectively as possible and choose a provider which is probably not yet infested, or which is not of interest for the NSA”.

From their perspective, the NSA surveillance scandal did not only affect IT companies but the U.S. economy in general (e.g. Buyer03). They even compared the events with

the George Orwell novel 1984 and argued that the NSA practices would harm the U.S. in the long run (e.g. Buyer03). One interviewee (Buyer06) gave the example of the wiretapping of the mobile phone of the German chancellor Angela Merkel (see Section 2.3.1) and argued that, although the phone must have been specifically protected, it was still possible for the NSA to record her phone calls. Buyer03 commented with a line attributed to Aesop, saying that “a liar will not be believed, even when he speaks the truth” (Mastro & Wells, 2014, p. 5). This statement makes clear that it could be difficult for U.S. cloud providers to win back the trust of their German customers.

Likewise, the cloud sellers experienced that the Snowden revelations caused uncertainty among German companies and had a negative impact on the trust of German companies in U.S. cloud providers (e.g. Seller03; Seller04; Seller05; Seller06; Seller08). They argued that the Snowden revelations caused anger and frustration at both sides, the German companies and the local sales representatives of the U.S. cloud providers (e.g. Seller06). Furthermore, they admitted that the U.S. cloud providers were not able to protect their customers in Europe from the USA PATRIOT Act and therefore the German companies would not trust public cloud solutions form U.S. cloud providers (e.g. Seller04).

According to the respondents, a general reaction among companies in Germany was that IT outsourcing and cloud computing projects were stopped, the companies started internal investigations about the security of their own data and were evaluating how they could protect themselves from access by the NSA. For example, Buyer06 reported that “all large enterprises are checking how safe they are from the NSA”. This also included a review of their IT service providers and external business partners. According to the buyers, the “overall sensibility increased” (Buyer07), and the Snowden revelations changed the overall perception of the German companies regarding data protection and IT outsourcing measures (e.g. Buyer08; Buyer11). To protect themselves against government spying, these companies therefore decided to keep their data either on-premise or to only use data centres in countries that they considered safe (e.g. Buyer03; Buyer06; Buyer11). The interviewees argued that they could not trust someone who betrayed their trust before and reasoned that there was no guarantee that the U.S. government would not do this again. Moreover, according

to the respondents, it “will take years, if not decades” (Buyer03) to rebuild the trust they lost in U.S. companies and the U.S. government. As another cloud seller summarised:

> *“The demand was already low in Germany, and Snowden slowed it even more down. The number of people that said that giving data to other companies was a bad idea was already high. This caused an even bigger drawback on cloud adoption than in other countries.” (Seller08)*

The cloud sellers concluded that “the Snowden topic did have an impact on the business” (Seller03), that “the business slowed down in Germany” (Seller04), that “it depressed the cloud business” (Seller05) and that it was a “great drawback on the cloud industry” (Seller08).

It was also the extent of the surveillance monitoring and recording which was a surprise to the cloud sellers as well as to their customers which caused strong reactions from German companies such as stopping cloud computing projects (e.g. Seller08). This was especially the case with customers that were already cautious with adopting cloud technologies (e.g. Seller03). According to the sellers, the cloud business in Germany, which was already weak before, slowed down even more after the global surveillance disclosures. For example, Seller04 claimed that “the NSA revelations destroyed the trust” and that the public cloud computing business “was very weak already and slowed down even more” after the Snowden revelations. Likewise, Seller06 stated that “the cloud topic was already difficult in Germany before” but “Snowden reinforced this general distrust”. Moreover, as argued by Seller08, “there were always people who said that you cannot trust the U.S. government” and “Snowden proved that they were right and that everybody in the entire world was spied upon”. He added that “nobody expected that all the communication is recorded and monitored and that the agencies had the capacity to do that”. Consequently, according to some sellers, several German companies used the NSA scandal as a welcome excuse to stop all projects that involved U.S. cloud services. For instance, Seller01 claimed that, “for conservative customers, this is what they were waiting for”.

Overall, these findings indicate that both buyers and sellers observed that the global surveillance disclosures reinforced the distrust of German companies in U.S. cloud services. The discussion chapter will evaluate the impact of this circumstance on the trust of German companies in the U.S. government.

5.13 Economic espionage

Several respondents indicated that the risk of economic espionage was one of the main reasons why they did not trust U.S. cloud providers with their data. For example, Buyer01 stated that he considered "economic espionage as the greatest danger". They expressed their fear of economic espionage and about the fact that they did not know how high the risk actually was. As stated for example by Buyer11, "yes, there is that fear. We don't know". Another informant said:

> *„So of course, I have concerns, and this is my original fear in this topic. Fear is the wrong word, but rather… no, fear is the right word." (Buyer08)*

Consequently, they were constantly evaluating if there was any negative impact on their business if a third party would get access to their data (e.g. Buyer08). Furthermore, they "would consider it neither impossible nor unlikely that government agencies are supporting the economic interests of American companies" (Buyer07) and they doubted that the spying efforts of the U.S. intelligence agencies were only targeting terrorism. For example, Buyer03 stated that it was "hard to believe that the USA is only interested in terror prevention but rather it is relatively obvious that there is quite another matter behind it". They assumed that the U.S. agencies would give data collected in foreign countries to U.S. companies and claimed that "certain CIA activities were only undertaken because they served the U.S. economy" (Buyer03). Another buyer claimed that, in the past, "data demonstrably disappeared and was used by U.S. companies to their advantage" (Buyer04).

The key respondents argued that the U.S. government would serve economic interests and that they could therefore not rule out any activities regarding economic espionage (e.g. Buyer06). Moreover, they claimed that, in the past, the U.S. oil industry benefitted from the Iraq War and that they gained access to the oil reserves of the country. In their opinion, it was therefore not unlikely that the U.S. government would also support their economy by sharing information gained from intelligence activities (e.g. Buyer07).

Another possible scenario of economic espionage that was described by the interviewees was an international acquisition where a company would be in the bidding process for a certain firm and a U.S. company would know the bidding price because of information they received from an U.S. intelligence agency.

Some of the interviewees claimed that their companies were constantly being attacked by hackers and that malicious software has been found on the IT systems of their organisations. However, from their point of view, only large intelligence agencies had the financial and technological power to decrypt complex encryption keys. As a result, their companies decided not to save any confidential data at a U.S. cloud provider or any external provider. For example, Buyer03 stated that he will “certainly not save any business-critical information, such as data on development projects, data on the corporate strategy, data about key people like business managers, in the cloud but would always try to keep them locally”. It also seemed that the revelations by Edward Snowden further increased the fear of economic espionage. While the risk of economic espionage was for some companies merely a theoretical threat in the past, the sensitivity for this topic grew since the NSA surveillance scandal (e.g. Buyer04).

From the experience of the cloud sellers, economic espionage was an important topic that was regularly raised in conversations with their customers (e.g. Seller03; Seller06). They confirmed that “the fear exists” and that “the topic economic espionage is important” (Seller03). As maintained by Seller04, “many customers in the R&D area would never put this data in the cloud”. Similarly, Seller05 explained that “especially machine engineering, well, almost solely machine engineering, are addressing this issue and are clearly saying that the Americans are practicing economic espionage”. He added that, unfortunately, he did not have “a satisfactory answer for that”.

A common belief expressed by several IT managers was that the concerns regarding economic espionage were largely a matter of the sector a company was in. For example, from the point of view of the IT manager of the advertising business, the risk of economic espionage related to public cloud computing was relatively low for his company (Buyer02). However, from the point of view of several key respondents, the manufacturing industry, the automotive sector and the automotive supplier industry were especially at risk of economic espionage (e.g. Buyer04; Buyer09; Buyer10).

The cloud sellers agreed that it was particularly the companies which had more intellectual property to protect which were more afraid of economic espionage (e.g. Seller04; Seller05). A prominent example was the automotive industry:

> *"Automotive industries have a great fear of economic espionage because they have the fear that their knowledge can be used by competitors in other countries. They fear that the U.S. government through the anti-terror law can access the data but also for getting competitive advantages." (Seller08)*

One cloud seller mentioned that the latest international lawsuits against the Volkswagen Group would increase the fear that international intelligence agencies would use company insights to file an action against foreign companies and thereby promote the domestic market (e.g. Seller08).

Nevertheless, the local sales representatives of the U.S. cloud providers argued that it would be dangerous to assume that company data stored in the local data centres of German companies or other data centres in Germany would be better protected from hacker attacks and economic espionage (e.g. Seller06). They claimed that the security measures of large cloud providers would be more sophisticated and hence provide a higher level of data protection. They recommended that cloud customers should use encryption technology to be sure that no information can be accessed from outside their company (e.g. Seller07). The relationship between the fear of economic espionage and the trust in the U.S. government will be explored in more detail in the discussion chapter.

5.14 U.S. government reactions

From the point of view of the key respondents it would be most helpful if the U.S. cloud providers would not be forced to give customer data to the U.S. government agencies. They argued that this would help the U.S. cloud providers to convince more customers to use their services and increase their cloud services revenue (e.g. Buyer05). In their opinion, the current situation scared away customers outside the USA and the U.S. government could only rebuild trust by changing the current practices of the U.S. intelligence agencies.

This view was also shared by the cloud sellers. From their point of view, the U.S. cloud providers and other U.S. companies needed to intensify their efforts to convince the U.S. government that the current legislations would have a negative impact on the U.S. technology industry in general and cloud services in particular. The cloud sellers wished that "the U.S. government becomes less deeply involved" (Seller03) and argued that the current policy of the U.S. government would endanger several jobs in the cloud computing industry. Furthermore, they claimed that the U.S. government would not change anything without the pressure of the U.S. technology sector (e.g. Seller04; Seller05).

A common view amongst the IT managers was, however, that it was quite unlikely that the U.S. government would make substantial changes to their policies regarding their data collection practices. For example, Buyer02 reported that he could not "imagine that there will be a substantial change of the law which then causes a substantial improvement of trust". The interviewees claimed that the U.S. government did not see the NSA spying practices as a scandal and that their approach was defensive and arrogant. From their point of view, the U.S. government never actively prohibited those spying practices and only talked about spying incidents when they were no longer able to hide them. As one of the buyers explained:

> *"They could no longer hide it, and they have not really actively prohibited it and not acted proactively, no. The power interests are stronger. And the American arrogance." (Buyer06)*

Consequently, the participants believed that even if the U.S. government were to make any significant changes, it would take many years to restore the lost trust. Buyer04 decided that he "wouldn't trust them anymore" and therefore "sit back, wait 5-10 years" and see how much he can still find in the press about these issues. He added:

> *"It would require a radical turnaround of the American politics and then it would take 10 years until one can trust them again. I don't see any chance." (Buyer04)*

Moreover, a few participants questioned if the U.S. government was still in control of their intelligence agencies or if the spying activities were being kept secret from the U.S. senate and the congressional representatives. They were concerned that the intelligence agencies would act according to their own rules and would not be monitored or controlled by other institutions. As expressed by one of the IT managers:

> *"One does not even know if they are still in control or if they are just overdriven by people in the background, from the intelligence agencies. This is one more of these elements of uncertainty." (Buyer03)*

Likewise, the cloud sellers assumed that "a critical reflection of the legislation will not happen" (Seller04) and they had "doubt that there will be a change" (Seller07) to the current legal system. They explained that much trust had already been destroyed (e.g. Seller06) and that it was rather unlikely that there would be any group that could put enough pressure on the U.S. government to change the country's surveillance laws. Seller05 made unequivocally clear that "it would be best if the U.S. government would shut up". Another cloud seller commented:

> *"Unfortunately, I think that the likelihood is very low. I don't see any influence of privacy ambassadors or civil rights activists." (Seller08)*

Taken together, almost all interviewees stated that they lost their trust in the U.S. government which had direct implications on their trust in the U.S. cloud providers. This relationship will be delved into in more detail in the discussion chapter. The following section will look at the opinions of cloud buyers and sellers on the initiatives by the German and EU governments regarding the global surveillance scandal and public cloud services.

5.15 German and EU government reactions

Most of the participants were unsatisfied with the way the German government had acted after more and more details of the NSA surveillance practices were reported by the press. They argued that the German government tried to downplay the Snowden revelations until they did not have any choice but to publicly address this issue. From their perspective, the German government did not represent the interests of the

German society but tried to cover the activities of the U.S. intelligence agencies to protect their relationship with the U.S. government. As noted by one of the IT managers:

> *„From my point of view, our government has put up a poor show and it seems like there is in many cases no interest in representing the interests of the German citizens but to step as little as possible on the toes of the Americans and somehow tolerate everything they do." (Buyer03)*

Moreover, some respondents claimed that the German government was actively involved in the spying efforts. In their opinion, the U.S. intelligence agencies would not have been able to access all the information they have collected in Germany without the help of their German partners. Furthermore, they did not see that the German government was making "any real attempt […] to clarify this matter" (Buyer04) and to educate the public about how the German intelligence agencies collaborated with the NSA (e.g. Buyer11). From their point of view, the German government did not act as it should have after the Snowden revelations and could have done much more to get to the bottom of this issue.

Additionally, in the opinion of most of the respondents, the German government was very much behind in terms of IT knowledge and capabilities. They did not believe that the German politicians had sufficient knowledge regarding Internet technologies and data privacy matters or that the German or the EU government would be able to take technical measures to prevent access by the U.S. intelligence agencies (e.g. Buyer08; Buyer09). The IT managers stated that the German politicians were "missing the skills" to "handle the issues of data protection, data rights and the Internet" (Buyer08) and that they would "probably go in the wrong direction" (Buyer09) if they get involved. One respondent (Buyer07) cited a famous statement of Chancellor Angela Merkel when she was asked about her response to the NSA surveillance scandal. Her answer was that the Internet was still "Neuland" (English: uncharted territory) and that they had to work with the U.S. government to restrict the data collection activities (Bundesregierung, 2013). However, a few respondents stated that they would still try to keep all their data in Germany because they had more trust in the "German data protection legislation […] than in the EU legislations" (Buyer03).

The local sales representatives of the U.S. cloud providers had a similar impression of the reactions by the German and EU authorities. Some interviewees commented that they had low expectations regarding any substantial changes to the legal systems. As one of the cloud sellers stated:

> *"The expectations were low and that proved right. Both the EU and the German officials didn't do a lot." (Seller08)*

From their point of view, the EU was not sufficiently critical of the U.S. government methods and "the pressure of the EU" was "too weak and uncoordinated" (Seller04). Others blamed the complex regulatory procedures of the EU and countries such as Germany for the slow adoption of new privacy legislations (e.g. Seller07). However, most of the cloud sellers wished that the period of uncertainty for the cloud industry would be over soon. For example, Seller05 stated that it was "about time that the Europeans come to an agreement with the Americans".

The buyers made some suggestions what the German or the European government bodies could do to improve the situation. Several interviewees wished that the German and European politicians were brave enough to tell the U.S. government that this was no way of dealing with a friend or partner. In their view, Germany and the EU should make it clear to the U.S. government that they were not willing to tolerate this practice anymore. From their point of view, putting pressure on the U.S. economy was the only way to make the U.S. government stop their surveillance activities. As one of the German IT managers explained:

> *"If they are not able to put pressure on them then I don't see any possibilities how they could help." (Buyer05)*

Likewise, Buyer03 explained that "this pressure can only come from economic indicators, incoming orders, sales revenue of U.S. companies, etc." and that "this is the only way to start a change process in the American government". One recommendation to put pressure on the U.S. government was to suspend the talks about the free trade agreement with the U.S. to apply pressure. Another suggestion was to support and rebuild the local IT and telecommunications industry in Germany and Europe to have an alternative to the IT solutions from U.S. companies. From their

point of view, the development of European hardware and software solution would be the only solution in the long run. They explained that it was the task of the German government to make sure that certain core technologies were provided by German companies. As commented by one of the IT managers:

> *"If you look at it, Siemens had computers, they had mobile phones, they hat computer chips, they had semiconductors, they had IT, Siemens successively sold all of it." (Buyer03)*

They further suggested that the German government could financially support German companies that were developing own IT solutions in areas such as encryption technologies. For example, Buyer04 stated that "every crisis also opens a new window of opportunity" and that "this would be a terrific opportunity for the German IT industry to ride the crest of this crisis". Seller06 demanded that "Germany should support more start-up companies and provide more investment capital" and requested that German "politicians should ask themselves how they can effectively secure Germany's position as a high-tech location". The discussion chapter will examine the reactions and technological expertise of German and EU government officials in more detail.

The following sections will present the findings related to the suggestions made during the interviews on how to improve the trust in U.S. cloud providers.

5.16 Data centre location

One of the most frequently mentioned measures how U.S. cloud providers could win the trust of German companies was to build a data centre in Germany. From the point of view of several German IT managers it was not so much of a problem that a U.S. company was their service provider, it was more important in what geography the data was stored. The key respondents explained that it was not an option for their companies to store any data outside of Germany (e.g. Buyer06). As stated by Buyer09, his company hat the "precondition" that "the data centres had to be in Germany". They argued that their companies required to keep their data in Germany because of the higher data protection and data security standards in Germany (e.g. Buyer06). The interviewees acknowledged that, from an economic point of view, IT service providers in other countries might be a better option. However, the economic

benefits had to be significant before their companies would store any data outside of Germany. Nevertheless, if all parameters were equal, they would still choose to have their data in Germany instead of another EU country (e.g. Buyer06).

Likewise, the local sales representatives of the U.S. cloud provider reported that a data centre in Germany was on top of their discussions with German clients and that one of the first questions of their customers in talks with them was about the location of the stored data. For example, Seller03 reported that the data centre location was "topping the list" and that "afterwards there are hardly any questions". They believed that a local data centre would build trust and drive cloud business in Germany. In their experience, the fact that their data would be stored in Germany was much more important than technical advantages such as improved network latency (e.g. Seller03; Seller04; Seller05).

Some IT managers acknowledged that the wish for a data centre in Germany might rather have psychological reasons. For example, one of the IT managers explained:

> *"In Germany, you just always have the feeling that it would be safer because it is located in Germany, but this is only a feeling and I don't think that this is somehow founded." (Buyer05)*

They recognised that a local data centre in Germany was a "step in the right direction, but it does not really solve the problem" (Buyer03). They argued that, even if the U.S. cloud provider had a data centre in Germany or another country of the EU, "they can still not guarantee that U.S. intelligence services have no access to the data" (Buyer04).

The cloud sellers agreed that in many cases the choice for keeping their data in Germany was based on the gut feeling of the decision makers of the German companies and not on legal necessities. As one of the cloud sellers commented:

> *"Local data centres are important. There is a difference in gut feeling when the data centre is on German soil, even if there is no legal reason to do that." (Seller08)*

They added that if the data was handled by German citizens that worked for German companies the trust would be even higher (e.g. Seller08). However, the local sales representatives noted that the U.S. cloud providers might not be able to provide the same level of functionalities and performance across all data centre regions. As one of the cloud sellers explained:

> *"Most customers would like to use a German data centre and have their data in Germany. But it might reduce the functionality and scalability of the solution." (Seller07)*

According to the sellers, the costs of cloud services from a local data centre in Germany could also be higher than from data centres located in the U.S. or in other larger markets (e.g. Seller06). These findings suggest that the location of the data centre is one of the variables that could influence the trust in U.S. cloud services. This relation will be further explored in the discussion chapter.

5.17 Legal proceedings

Another suggestion that came from some of the respondents to improve the trust of German companies in U.S. cloud providers was to file an action against the U.S. government regarding the practices of the U.S. intelligent agencies. They believed that this approach would create trust because potential customers would see that the U.S. cloud providers would be on their side and fight for their privacy rights (e.g. Buyer03). As one of the buyers commented:

> *"This creates trust because the customer can see that Microsoft is not simply giving data away but that they argue in the interests of the customers and support their causes. I believe that this already helps a lot." (Buyer05)*

Others argued that it was a step in the right direction that the U.S. cloud providers took a stand for data privacy and were trying to protect the data of their customers. However, they explained that it was difficult for them to know if these legal actions against the U.S. government were meant to protect their customers or if they were merely "a press or marketing gag" (Buyer06). For example, one of the IT managers stated:

> *"I believe that this is in any case the right approach. However, as I tried to say before, I wouldn't be able to distinguish or tell if this was part of a marketing campaign or if this was really serious about that." (Buyer04)*

In the opinion of the cloud sellers, it was important that the U.S. cloud providers showed interest in the concerns of the German companies and acted accordingly (e.g. Seller04). They explained that their German customers would welcome any initiatives of the U.S. cloud providers to prevent U.S. government agencies from accessing their data (Seller05). As one of the cloud sellers argued:

> *"The customer is happy that we go this way and enforce whatever we can to stop this access and data. This is what they expect from us." (Seller07)*

However, not all German companies were equally interested in these legal actions by the U.S. cloud providers. One of the cloud sellers (Seller08) reported that he would have expected a higher interest by his customers in these measures.

The discussion chapter will evaluate if and how U.S. cloud providers can improve the trust of German companies in their services by filing an action against the U.S. government.

5.18 Cloud computing contracts

The IT managers of the German companies also criticised the current contractual frameworks. From their experience, many cloud providers only offered contracts with a jurisdiction in the U.S., England or Ireland. They criticised that German companies who wanted to do business with U.S. cloud providers often had to sign a contract under the jurisdiction of these countries. Additionally, these contracts were often too complex and required external consultancy (e.g. Buyer09). They argued that the U.S. cloud providers would create contracts "that most company lawyers do not really understand, but where you have to consult a specialist" (Buyer02) to be able to sign any agreements.

Additionally, the key informants reported that the U.S. cloud providers were not willing to make any changes to their standard contract terms and conditions. They claimed

that they would have to either sign the standard contracts or choose a different provider. For example, one of the IT managers explained:

> *"If you have contracts with an American company, by virtue of its size, it won't even change a comma in the terms and conditions for us. Either you sign, or you can forget it." (Buyer09)*

The interviewees demanded that "the legal requirements have to be at the same level" as their on-premise infrastructure contracts (Buyer06) and argued that only U.S. cloud providers who would listen to the needs of their customers and act accordingly would be successful on the German market (e.g. Buyer08).

However, some respondents did not believe in any contractual agreements anymore. From their point of view, contractual agreements and written guaranties of the U.S. cloud providers were not worth anything unless legal frameworks like the USA PATRIOT Act were changed (e.g. Buyer03).

The cloud sellers admitted that the German law was different from the U.S. legislation and that the standard contracts of some of the U.S. cloud providers did not meet the requirements of many German companies. They reported that their customers required that contracts needed "to be made up according to German law" (Seller01), in German language and with a jurisdiction in Germany (e.g. Seller08). As stated by Seller03, the wish of his customers was that "jurisdiction shall be in Germany". The local sales representatives of the U.S. cloud providers acknowledged that the German law was particularly consumer friendly with "unlimited liability" (Seller07) and that "American companies don't like to do that" (Seller02). As summarized by one of the cloud sellers:

> *"My feeling is that customers want to have everything local. The less they have to deal with the bigger their interests are in cloud." (Seller08)*

They also stated that it was important that the U.S. cloud providers had the legal competence to talk to the German customers about local juridical requirements and proactively address these issues. In their experience, the U.S. cloud providers

underestimated the specific needs of the European market and did not like to change their services and contracts to meet these requirements (e.g. Seller02).

In summary, these findings show that the buyers required certain changes to the current cloud contracts that could potentially increase their trust in U.S. cloud services. This proposal will be further detailed in the discussion chapter.

5.19 Data encryption

Another request from several of the respondents was that the U.S. cloud providers should offer secure encryption methods, preferably with the option that the German companies could use their own encryption keys. For example, one respondent stated:

> *"Yes. I think encryption is another mechanism. It is definitely a mechanism for that." (Buyer11)*

Some of the German companies were already using encryption technologies to protect their data and stated that they had "a policy in place which says that every email which is somehow strategically important or contains personnel data or such things has to be encrypted" (Buyer05).

However, in the opinion of other respondents, the NSA had many technical possibilities and "eventually a clever person with the necessary funds and the necessary working environment will find a hole" (Buyer01). They claimed that it was not possible to completely secure the data with encryption and that this was like the "race between the hare and the hedgehog" in the German fable (e.g. Buyer01). Additionally, the IT managers argued that data was no "haptic good" and that it was therefore difficult to find out or prove if it was stolen (e.g. Buyer07).

The local sales representatives of the U.S. cloud providers agreed that data encryption was "a big talking point" with their customers and would "help a lot with building trust (Seller05). However, they also explained that data encryption "creates new challenges for both parties" (Seller06). They further elaborated that any end-to-end encryption with third party tools could possibly cut off some features of SaaS products such as indexing and search functionalities. As one of the cloud sellers explained:

> *"It's a huge request by the customers. Sometimes customers would like to encrypt everything. But if they encrypt on their level we cannot work with the data and the applications do not work as designed." (Seller07)*

However, as one of the cloud sellers commented, "encryption is a very hard topic and U.S. cloud providers should make it much easier for their customers to use it in order to gain trust" (Seller08). Nevertheless, as warned by Seller01, cloud data encryption should not be seen as "a free ticket for the cloud consumer but a model of dual responsibility" where both parties have to invest in making data transmissions, processing and storage secure.

These findings suggest that both buyers and sellers identified encryption technologies as a potential way to increase the trust of German companies in U.S. cloud providers. However, as pointed out by some of the sellers, this approach might result in reduced cloud service functionalities. This potential trade-off will be examined in more detail in the following discussion chapter.

5.20 Summary

This chapter presented the findings of this study and highlighted the themes that emerged from the analysis. In general, the concept of **trust played an important role** for the German companies when making purchase decisions for public cloud services and the relevance of trust in buyer-seller relationships was clearly supported by the current findings. Both buyers and sellers agreed on the proposition that trust was an essential component in social life and business relationships in general and in cloud computing services in particular. With regards to cloud computing, the research participants argued that the nature of a public cloud service would imply that they could not verify themselves that no third party would ever be able to get access to their companies' data or completely protect themselves against other damages that could occur to their businesses. Hence, the buyers wanted a business partner whom they could trust and who would take all necessary measures to ensure that their data and intellectual property was protected.

The **cultural differences** between the U.S. and Germany and the potential impact on the cloud adoption by German companies was one of the key themes that emerged

from the data analysis. The cultural and historical background of the German buyers were potentially one of the key reasons that made them particularly careful about data privacy and data security issues. The findings suggest that there is an association between the cultural differences between the U.S. and Germany and the adoption of U.S. cloud computing services by German companies.

An unexpected finding that emerged from the data which spanned across other research objectives was the influence of the **sector and size** of the company on the cloud adoption by German companies. The initial assumption at the beginning of this research was that the sector a company was operating in had no or only a negligible influence on the willingness of a company to adopt U.S. cloud services. The findings revealed, however, that this assumption was incorrect and that certain sectors were noticeable more cautious in using public cloud services. The reasons behind this cautiousness varied between sectors. The insurance industry was for example restricted by legislation to use public cloud services and the automotive sector was on the other hand afraid of economic espionage threats and did not trust U.S. cloud providers with their data.

Most of the German companies interviewed in the current research acknowledged the technological and business benefits of public **cloud computing technology** as described in the background chapter and a few buyers even called themselves strong supporters of the cloud. The cloud sellers reported that the buyers would usually trust the product/service itself and that most of their customers would recognise the technological capabilities of large cloud providers. This finding indicates that a lack of confidence in the performance and reliability of cloud computing systems was probably not slowing down cloud usage by German firms.

Both buyers and sellers agreed on the view that **U.S. cloud services** were superior to cloud computing technologies offered by EU or German providers. According to the buyers, there was no solution on the German or EU market that could for example compete with some of the SaaS productivity services offered by U.S. cloud firms. The cloud sellers added that most of their customers would see U.S. cloud providers as clear market leaders and would acknowledge the technological edge and scale of the U.S. solutions.

The respondents acknowledged the existence of **shadow IT** cloud services and the potential risks involved. The buyers reported that employees would introduce consumer information technology to the workplace to exchange data with colleagues and external parties and that this was a known issue although it was not compliant with their IT policies. Historically, the IT departments of the German companies would provide the necessary productivity tools to all employees but, according to the respondents, there was a growing number of public cloud services that was used for daily work activities.

Most of the German companies of the current research did not believe that the **U.S. cloud provider** companies were actively involved in the NSA surveillance activities. The key informants of the German companies argued that the U.S. cloud providers would not do anything which has a negative consequence for their business and that U.S. technology companies could have collected customer data for many years in the local data centres of the German companies if they wanted to. Nevertheless, the buyers explained that they did not know if the U.S. cloud providers were forced by the U.S. government to give them access to customer data and that the German companies could therefore not trust the U.S. cloud providers. Since the U.S. cloud providers could not guarantee that the U.S. government would not get access to customer information, the risk of storing their data with a U.S. cloud provider outweighed the technological and financial benefits that U.S. cloud providers might offer. A few respondents even claimed that they would replace all U.S. technology products in their companies if they could. Hence, the trust in the U.S. cloud provider company was displaced by the distrust in the U.S. government.

Buyers and sellers reported that **German cloud providers** tried to take advantage of the NSA surveillance scandal by advertising that their cloud data centres would be inaccessible by U.S. government agencies. The German companies stated that they themselves and their customers would have more trust in German cloud providers than in cloud providers from the U.S. or from other European countries.

However, most of the key informants of the German companies revealed that they preferred to keep their data in their local on-premise data centres in a **private cloud** setup. The reasons why the companies preferred to keep their IT in their own data centres varied. Some argued that public cloud solutions could not provide a higher

level of security and data privacy, others explained that the cost savings of public cloud services were not convincing or that their local staff could provide a better IT service to them. The cloud sellers acknowledged that most German companies favoured on-premise IT solutions in their local data centres and even admitted that they could not guarantee that the NSA would not get access to data stored in the cloud. This statement confirms that buyers may have a valid reason for their suspiciousness since the cloud sellers could not completely rule out the possibility of government access to customer data.

All in all, it can be said that the IT managers of the German companies were undecided about their trust relationship with the local sales representatives of the U.S. cloud providers. On the one hand, they argued that they did not need the help of a **local sales representative** of the U.S. companies to come to a decision about cloud services and that they could not trust the statements of those salespeople because they were uninformed about the details of any surveillance activities driven by U.S. intelligence agencies. The buyers also claimed that the local sales representative did not have any decision powers and that they had to contact the company's headquarters in the U.S. in order to get any binding commitments.

However, on the other hand, the IT managers demanded for local staff of the U.S. cloud providers that could speak their language and was trained to their **market and sector** specific needs. The buyers argued that it was the responsibility of the U.S. cloud providers to hire and train salespeople who would understand the German market and its specific industry in order to support their business. The seller respondents echoed the statements of the buyers and claimed that especially enterprise customers demanded a local contact person that spoke their language and that large German companies would not buy cloud solutions without a personal meeting with a local sales representative.

The first finding revealed that the **global surveillance activities** of the U.S. intelligence agencies destroyed the trust of German companies in U.S. cloud services and slowed down the public cloud computing adoption in Germany even more. The global surveillance activities revealed by Edward Snowden caused extensive media coverage in Germany and led to great uncertainty in the general public. Several

respondents reported that their companies stopped their cloud computing projects and started investigations about the security of their data.

One of the key concerns raised by the German companies was an increased likelihood of **economic espionage**. The IT managers feared that the U.S. government would support the local economy by providing U.S. firms with German company secrets collected through U.S. intelligence agencies. Since the German economy is heavily invested in the production of machinery, automobiles, electrical equipment and chemicals, the theft of intellectual property and non-submitted patent applications could cause substantial harm to those businesses. Consequently, these sectors shy away from saving confidential data in a public cloud infrastructure.

The respondents stated that it would help if the **U.S. government** would change the legislation and make a clear statement that U.S. cloud providers could not be forced to hand out customer information to government agencies. They argued that this would help convince more customers to use U.S. public cloud services and increase the revenue of the providers in Germany. From the point of view of the respondents, the current situation would scare away customers outside the U.S. and trust could only be restored by limiting the scope of the U.S. intelligence agencies. However, at the same time, the German companies found it unlikely that the U.S. government would reduce their surveillance activities. Moreover, even if the U.S. government would make substantial changes to their law, it might take many years for the U.S. government and U.S. companies to win back the trust of the German businesses.

However, not only the U.S. government forfeited the trust of German companies but also the **German and EU government** officials disappointed the buyers with their statements and actions. The statements of the IT managers of the German companies and the sales representatives of the U.S. cloud providers showed that they did not deem the reactions of the German and EU government officials to be sufficient. The buyers claimed that the German government tried to downplay the Snowden revelations until they did not have any choice but to publicly address this issue. From their perspective, the German government did not represent the interests of the German society but tried to cover the activities of the U.S. intelligence agencies and the activities of their own intelligence departments. The buyers argued that the German government did not educate the public about how the German intelligence

agencies collaborated with the NSA and that they assumed that they were closely working together. The IT managers wished that the German government would take a clear position by protecting their citizens from foreign government surveillance activities and by financially supporting German companies that were developing cloud computing services.

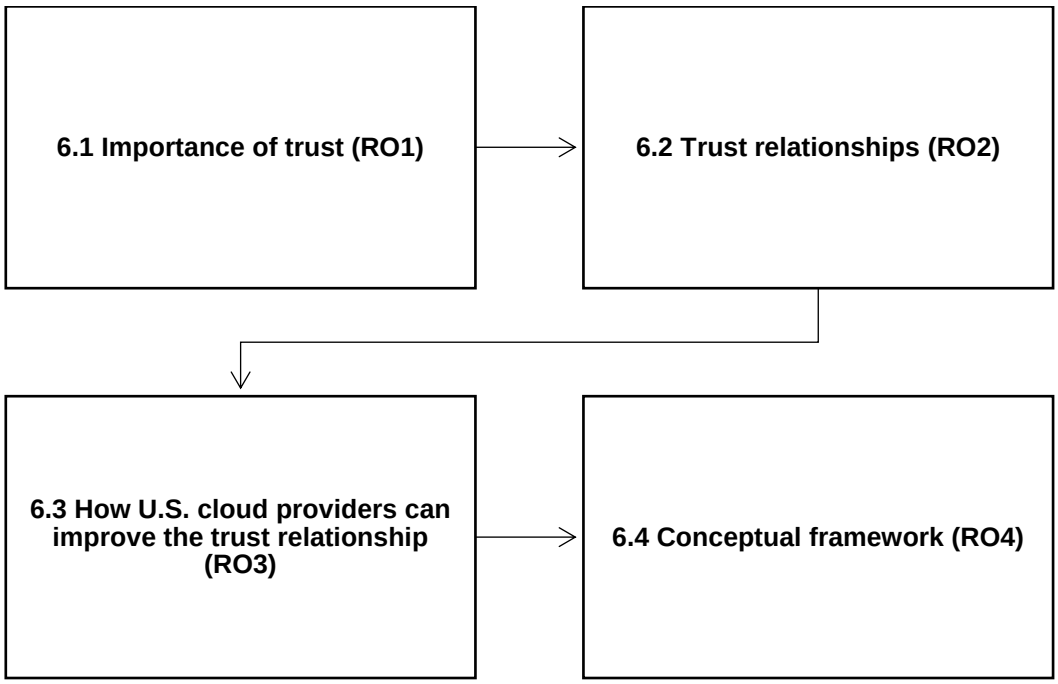
Finally, the buyers made several suggestions how U.S. cloud providers could potentially improve the trust in their services. The first suggestion from the German companies to the U.S. cloud providers was to build a **data centre in Germany** and store all data of their German customers in Germany. The second demand of the German companies was that the U.S. cloud providers should take **legal proceedings** against the requests of the U.S. government to hand over data of their European customers. Request number three was to have all **cloud computing contracts** with U.S. cloud providers in German language and under German jurisdiction. The last repeated recommendation by the IT managers was that U.S. cloud providers should offer secure but easy to use **data encryption** technologies that allow their customers to provide their own encryption keys.

Together these results provide important insights into the role of trust in the business relationship between German companies and U.S. cloud providers. The notion of trust was a key element throughout the reporting of the findings and a connecting link between the themes. The following chapter will discuss these findings with regard to the literature reviewed in Chapter 3.

6 Discussion

Each main section in this chapter addresses one of the objectives of the current research. The first section discusses the importance of the concept of trust for German companies for the adoption of public cloud computing services from U.S. cloud providers (RO1a) including the impact of cultural differences between the U.S. and Germany (RO1b) and the influence of the sector the company is operating in (RO1c).

The next main section explores the trust relationship between German companies and U.S. cloud products (RO2a), U.S. cloud provider companies (RO2b), the local sales representatives of the U.S. cloud providers (RO2c) and the U.S. government (RO2d).



The third main section discusses four ways how U.S. cloud providers can improve the trust relationship with German companies and the last main section aggregates the results in a conceptual framework.

6.1 Importance of the concept of trust for cloud adoption (RO1)

The first research objective of this study was to analyse the perspectives of the buyers and the sellers on the importance of trust for German companies for the adoption of public cloud computing services from U.S. cloud providers (RO1a), the impact of the cultural differences between Germany and the U.S. on trust and public cloud adoption (RO1b) and the influence of the sector of a German company on trust and public cloud adoption (RO1c).

The section that follows will discuss the importance of trust for German companies for social life and business in general and for cloud computing adoption in particular.

6.1.1 Importance of trust (RO1a)

The key respondents highlighted the importance of the concept of trust for business relationships in general and for cloud computing purchase decisions in particular. This is in line with the literature on trust by sociologists and economists reviewed above. For example, Weber (1968, p. 114) reasoned that the exchange of goods was only possible “on the basis of far-reaching personal confidence and trust", Hirsch (1977, p. 78) argued that trust was “necessary for the success of economic transactions" and Zucker (1986, p. 56) stated that trust was "vital for the maintenance of cooperation in society and necessary as grounds for even the most routine everyday interactions".

Other respondents even maintained that trust was a vital component for humanity. The literature on the importance of trust reviewed in Section 3.1 mostly agreed that the notion of trust was essential for social interaction. For example, Blau (1964, p. 99) argued that trust was "essential for stable social relationships", Lewis and Weigert (1985b, p. 968) maintained that trust was "indispensable in social relationships" and Golembiewski and McConkie (1975, p. 131) claimed that there was “no single variable which so thoroughly influences interpersonal and group behaviour as does trust".

Moreover, the findings from the interviews indicated that trust played an important role in the decision of German companies regarding the adoption of public cloud computing services. This view was shared between both the buyers and the sellers. This finding corroborates the ideas of Ganesan (1994) and Sako (1998), who suggested that plays a key role in determining the long-term orientation of both buyers and sellers and was associated with supplier performance.

Fragility of trust

Another aspect mentioned by the interviewees was that it could take a long time to build up trust but that it would only take a brief time to lose it again. This view confirms the ideas of philosophers cited in Section 3.2.1 such as Baier (1986, p. 242), who described trust as a "fragile plant" and suggested that "trust is much easier to maintain than it is to get started and is never hard to destroy". Case studies on organisational failures and trust repair reported similar results. The researchers concluded that "trust failures typically take years to resolve, and can be both debilitating and very costly" (Dietz & Gillespie, 2012, p. 36). Other studies examined under which conditions trust is broken and suggest remedial actions to repair the trust relationship. For example, Lewicki and Bunker (1996, p. 131) recommended as "first steps in reciprocal trust repair" to (1) recognize and acknowledge that a violation has occurred, (2) determine the nature and causes of the violation and admit that one has caused it, (3) admit that the act was destructive, and (4) accept responsibility for the effects of one's actions. In case of the global surveillance activities, the U.S. cloud providers acknowledged that the U.S. government issued National Security Letters (NSLs) that forced them to provide customer data to U.S. intelligence agencies, the U.S. cloud providers named the NSLs and wiretapping as causes, they admitted that the act was destructive for their business and accepted the responsibility to protect the data of their customers.

However, as argued by the buyer respondents, the U.S. government did not accept any responsibility and downplayed the incidents. Therefore, it might be difficult for the U.S. cloud providers to rebuild the trust with their customers without any help from the U.S. government. Similarly, Tomlinson, Dineen, and Lewicki (2004) have suggested that violators should always admit culpability and apologize where appropriate. Nevertheless, not all researchers agreed that apologizing is the best approach in all situations. For example, Kim, Ferrin, Cooper, and Dirks (2004) found that apologies are less effective for integrity violations but helpful for competence-based violations and Bottom, Gibson, Daniels, and Murnighan (2002) argued that explanations and apologies can only be effective to a certain degree and that substantive amends have significantly more positive effects. Furthermore, Nakayachi and Watabe (2005) demonstrated that voluntary hostage posting raised the perceptions of trustworthiness whereas Dirks, Kim, Ferrin, and Cooper (2011) found that both penance and apologies increased trust after a violation.

Therefore, it might help those U.S. cloud providers who actively participated in any surveillance activities to apologize for their involvement. However, those U.S. cloud providers who have been unknowingly used for the data collection activities might not have anything to apologize for and would need the U.S. government to admit the wiretapping activities and promise to stop these methods instead. This is, however, nothing that the U.S. cloud providers can decide for themselves and where they can only try to influence the U.S. government to change the legislation and stop any surveillance activities that are harmful for their business.

6.1.2 Impact of the cultural differences (RO1b)

One of the key themes that emerged from the data analysis was the cultural differences between the U.S. and Germany and the possible impact on the cloud adoption by German companies. The importance of trust, as discussed in the previous section, in combination with the globalisation of goods and services, highlight the need to understand how national culture impacts trust-building (Doney et al., 1998; Sako & Helper, 1998). Triandis (1972) reasoned that since values and norms vary across cultures, the process of trust building probably also depends on culture. In a similar way, Dyer and Chu (2000, p. 279) maintained that the “levels of supplier trust differ by country”. For example, a buyer could distrusts the supplier or it’s representative “for reasons related to differences in cultural alignment” (Handfield & Bechtel, 2002, p. 377). Although trust may form in many ways, national culture and social norms have a strong influence on whether and how trust is established (Hofstede, 2003a). Likewise, Young-Ybarra and Wiersema (1999, p. 456) found that “the existence of shared values between the partners is positively related to trust”. However, as maintained by Wright and Ehnert (2010, p. 111), “privileging a cultural perspective when understanding social phenomena can only ever result in a partial story of human organizing, never the whole story”.

From a constructivist point of view, culture may be seen as “being made up of relations, rather than as a stable system of form and substance” (Yousfi, 2010, p. 233). In other words, individuals can have multiple cultural memberships from various social identities (S. C. Schneider & Barsoux, 2003) and national culture is just one facet of culture that would most likely work in concert with others such as ethnicity, industry or profession. Yousfi (2010) suggests that every person embodies a combination of

cultural, personal and social experience and, therefore, any communication could be seen as intercultural. According to the author, the influence of national culture on individual action and the trust-development process is a complex process which is influenced by various external factors and therefore difficult to predict and generalise.

As maintained by Wright and Ehnert (2010), constructivist researchers hold certain assumptions about the world that influence their research. The implication of this "for research into trusting across cultures is that there is no ultimate element at the heart of trust to be revealed through deductive inquiry" (Wright & Ehnert, 2010, p. 121). The authors argued that trusting is too open ended and fluid to have a central feature that is consistent across context and that the pursuit of antecedents would be a misguided journey from the perspective constructivist researchers. Furthermore, as stated by Wright and Ehnert (2010, p. 124), "social constructionists should only ever claim to tell a partial story of trusting across cultures, not *the* story."

The current research will discuss the cultural themes from the interviews using the Hofstede's cultural dimensions and compare the results with previous studies. As mentioned in the literature review chapter, not all studies on culture were conducted in a business to business context and people might show a different behaviour in a business situation than in a personal context. However, since companies are run by humans, their personal cultural background also has an influence on their professional work decisions.

6.1.2.1 Individualism

The individualism dimension characterises "the degree of interdependence a society maintains among its members" (Hofstede, 2018, p. 2). It is essential to cultural systems (Allik & Realo, 2004; Oyserman, Coon, & Kemmelmeier, 2002) and applied across disciplines including anthropology, business, history, philosophy, psychology and sociology (Triandis, 2018). It is the most studied dimension in information systems research (Posey et al., 2010) and "about one-third of recently published studies cited [individualism/collectivism] as at least a partial explanation of observed cross-cultural differences" (Kâğıtçıbaşı, 1997, p. 3).

Even though both the U.S. and Germany represent individualistic cultures, this dimension is far more pronounced for the U.S. culture (Krasnova & Veltri, 2010).

However, the individualism index of Germany (67) is still considerably higher than the world average (43) (Hofstede, 1991). Besides, Lind and Earley (1992) argue that even the most individualist individuals care about collectivistic group matters. Germany is described as a “truly Individualist” society with a strong belief in the ideal of self-actualization. The communication style in the German society is among the most direct in the world following the model to be “honest, even if it hurts” (Hofstede, 2018, p. 2). This can also be said about the answers that the respondents gave in their interviews. Both buyers and sellers came straight to the point and gave answers that could be described as forthright or blunt. As detailed in the findings chapter, the respondents also commented on the high level of individualism of the U.S. culture. For example, the buyer emphasised that the U.S. government never actively prohibited their spying practices and only talked about the spying incidents when they were no longer able to hide them. Although the local sales representatives of the U.S. cloud providers mostly held the German companies responsible for the slow cloud adoption in Germany, they acknowledged that the U.S. culture would contribute to the situation. The sellers maintained that the U.S. would primarily focus on their national interests and on protecting the country from external threats without considering the interests of other countries. Moreover, the buyers claimed that the U.S. companies would not know much about the culture in foreign countries and where certain countries are located. The present findings seem to be consistent with other research which found that the U.S. is rated as one of the most individualist cultures in the world. The expectation in the U.S. society is, according Hofstede (2018), that people look after themselves and should not rely on authorities for support. Additionally, U.S. Americans are said to be used to interacting or doing business with people they don’t know well. Likewise, Triandis (2001, p. 909) argues that individualist cultures “give priority to their personal goals” and act accordingly to achieve them. This view was also shared by the buyers and sellers of the current research.

According to the buyers, the cultural differences between the U.S. and Germany was a key reason why they did not believe in considerable changes to the U.S. law anytime soon. These findings further support the idea of Hofstede (2003a), S. C. Schneider and Barsoux (2003) and Fukuyama (1995) who maintain that cultures are highly resistant to change. As argued by Gannon (2004, p. 15), the Internet has not resulted in a “global village” but has led to “as much differentiation as integration and possibly

more differentiation". He added that major technological changes have a greater influence on culture only in the later stages of maturation. Likewise, R. Srinivasan (2017, p. 6) argued that it was an "incorrect prediction" that the world would become a global village because of the Internet. In case of public cloud computing services for enterprise customers, this would mean that the service was not seen in the same way in every culture and that cloud providers should take the cultural specifics of each target market into account.

In-group and out-group

Another aspect of the individualism dimension is the differentiation between in-group and out-group members. Dinev et al. (2006) maintained that members of more collectivistic cultures differentiate stronger between in-group and out-group members than highly individualistic cultures. Highly individualistic cultures, on the other hand, are more likely to trust people in general, including strangers who are not in one's social group (Inglehart, Basanez, Basanez, & Moreno, 1998; Yamagishi & Yamagishi, 1994). It could therefore be argued that German companies see U.S. cloud providers as foreign and out-group entities and develop less trust in those companies than in German providers or their own private data centres. This view of German companies in respect to out-group U.S. cloud providers could hence contribute to the distrust in U.S. cloud services. Therefore, German companies could see their own private datacentre and German cloud providers as in-group and U.S. cloud providers as out-group entities. However, as stated by Triandis (2001, p. 909), it should not be assumed that all members of an individualistic or collectivistic society have all the characteristics of this culture but that "people sample from both the individualist and collectivist cognitive structures, depending on the situation".

Information sharing

Furthermore, the buyers in the current research commented on the different information sharing practices between the U.S. and Germany (e.g. salary and population census). The individualism dimension was also associated with the willingness to information sharing. As argued by Bellman et al. (2004), Dinev et al. (2006) and Miltgen and Peyrat-Guillard (2014), culture largely determines privacy concerns. Krasnova and Veltri (2010) found that the amount of information that the U.S. participants were willing to disclose on social network services was significantly

higher than the data shared by the German respondents. The authors explained this finding with the lower individuality scores of the German culture, who, from their point of view, would “be more likely to suppress their emotions” (Krasnova & Veltri, 2010, p. 9).

Additionally, Krasnova and Veltri (2010) found that their German respondents were much more likely to hide their personal information by changing their real names to nicknames or publishing only their first names. As highlighted by Hern (2018b), the use of pseudonyms was a popular way of German Facebook users to cover their real identity and protect their privacy. In February 2018, following a lawsuit brought by the Federation of German Consumer Organisations (Verbraucherzentrale Bundesverband – vzbv), the Berlin Regional Court decided that “Facebook’s requirement that users must use their real names was a covert way of obtaining their consent to the use of this data, and that alone was reason enough to rule it unlawful” (VZBV, 2018, p. 2). This difference in the information sharing behaviour between U.S. and German Internet users can be seen as another example of the influence of national culture on privacy preferences and trust in Internet service providers. Other studies came to similar results. According to Ting-Toomey (1991), members of highly individualistic cultures are more comfortable with data disclosures and have fever privacy concerns. The IBM Multinational Consumer Survey highlighted in Section 3.6.2 found that Americans were about half as concerned about data privacy issues as Germans (Harris Interactive, 1999). Likewise, Maynard and Taylor (1996) found that U.S. students were less concerned about data privacy than Japanese students (who have an individuality score of 46).

However, in contrast, other studies such as Milberg et al. (2000) and Posey et al. (2010) indicate that cultures with higher individuality scores are more concerned about data privacy than collectivistic cultures. For example, Bellman et al. (2004, p. 3) argued that collectivist societies have “a greater acceptance that groups, including organizations, can intrude on the private life of the individual”. Similarly, Miltgen and Peyrat-Guillard (2014, p. 116) found that European citizens “from collectivist countries express more trust and are less reluctant to disclose information than are those from individualistic countries”. Even the study of Krasnova and Veltri (2010) showed inconsistent results in terms of data privacy behaviours. In several instances the U.S.

participants had higher privacy concerns than the Germans. For example, 22.8% of the U.S. Facebook users stated to be “very much concerned about the fact that their information could be used in a way they did not foresee” compared to 10.2% of the German participants (Krasnova & Veltri, 2010, p. 5). The authors speculated that U.S. social network users, due to higher individualism, may be more concerned because they could fear that it this information could be used against them and to the advantage of someone else.

These contradictory results “suggest an ongoing discussion about whether individualistic national cultures are more or less concerned about privacy” (Miltgen & Peyrat-Guillard, 2014, p. 107) and that “the strength of the negative relationship between privacy concerns and self-disclosure is still to be examined in an intercultural setting” (Krasnova & Veltri, 2011, p. 892). Hence, even though individualism may “play a role in the formation of privacy concerns, the role of this cultural dimension is ambiguous” (Krasnova & Veltri, 2011, p. 892). The current research could not resolve this conflict but contribute to the number of studies that examine the role of the individualism-collectivism dimension regarding sharing personal information. Additional research will be necessary to find answers to the question why past studies show contradictory results regarding the relationship between data privacy and individualism.

6.1.2.2 Uncertainty avoidance

Hofstede (2018) defined uncertainty avoidance as “the extent to which the members of a culture feel threatened by ambiguous or unknown situations and have created beliefs and institutions that try to avoid these”. Uncertainty avoidance addresses the concept of risk preference and risk-reducing strategies (Hofstede, 2003a). The extent to which cultures try to mitigate uncertainty is determined by their tolerance for unclear, unpredictable or unstructured situations (Singh, 1990). According to Hofstede (2018), Germany is on the high end of uncertainty avoidance countries with a strong preference for deductive approaches in thinking, planning and presenting. In the German culture, all details are equally important, and a project needs to be well-thought-out in order to proceed. As described by Hofstede (2018), Germans need to get a systematic overview of a topic before making decisions and compensate for their uncertainty by strongly relying on expertise. Consequently, “Germans are expected to

be more risk averse, feel threatened by uncertain conditions, prefer the tried and tested ways over new methods" (Krasnova & Veltri, 2010, p. 2) and show strong faith in institutions (Krasnova & Veltri, 2011). The following sections will discuss the cultural traits with regard to uncertainty avoidance from the findings of the current research.

Risk taking

As described in Section 3.2, the involvement of risk is a prerequisite for any trusting situation. Therefore, uncertainty and uncertainty avoidance are directly related to trust and the sources of risk in trusting situations are mostly related to uncertainty about an outcome (Doney et al., 1998). Lewis and Weigert (1985b, p. 970) stressed the need for uncertainty, because "if one were omniscient, actions could be undertaken with complete certainty, leaving no need, or even possibility, for trust to develop". According to the sociologists Johnson-George and Swap (1982, p. 1306), the "willingness to take risks may be one of the few characteristics common to all trust situations". Likewise Luhmann et al. (1979, p. 42) claimed that a "fundamental condition of trust is that it must be possible for the partner to abuse the trust". Other authors, such as Deutsch (1958) and Zand (1972), came to similar conclusions.

A cultural difference described by the respondents was that Germans wanted to understand everything before making decisions whereas the people from the U.S. would be more willing to take risks. This finding corroborates the ideas of Hofstede (2003a), who suggested that individuals in low uncertainty avoidance cultures tolerate risk more easily and do not have as much fear of the future (Hofstede, 2003a). In another study, H. Park (1993) finds that cultures with a high score of uncertainty avoidance have a higher insurance penetration. This finding can be interpreted as another confirmation that risk-averse individuals prefer risk-reducing behaviour. It could therefore be argued that the relatively low cloud adoption rate in Germany is part of the German attitude towards risk taking and uncertainty avoidance. Although the buyers acknowledged the business benefits of public cloud computing (see Section 5.4) and the superior technology of U.S. cloud providers (see Section 5.7), they still planned to invest in private cloud solutions in their own data centre instead (see Section 5.9).

According to Mauerer (2016, p. 2), the "try and error" and "just do it" mentality of U.S. citizens is frowned upon in Germany. This might be especially the case when the

decision involves legal matters such as storing company data including personal data and trade secrets in cloud services. The revelations by Edward Snowden have probably aggravated the situation. As stated by several sellers, the cloud business in Germany was already weak before the revelations and the global surveillance disclosures have reinforced this distrust.

Several buyers used the word “Angst” to describe the risk of economic espionage for their business when using U.S. public cloud services (see Section 5.13). Additionally, the cloud sellers argued that their customer would often rely on their gut feeling instead of having a fact-based discussion. The question arises, therefore, whether this general fear is an inherent part of the German culture. The term “German Angst” is internationally known and describes the pessimism, despondency and wariness in the German society (S. Bode, 2006). Germans are described as always fearing the worst and avoiding risks (Fersch, 2012). This German Angst is also cited as one of the reasons for the relatively low cloud adoption by German companies (Müller & Witmer-Goßner, 2015). It could therefore be argued that the reservations of German companies regarding public cloud services from U.S. cloud providers are not primarily based on actual facts but on a general mistrust and indefinable anxiety caused by their cultural influence. One explanation might be that cloud computing is a non-tangible good which makes it difficult for buyers to assess the risks involved in the purchase and the usage of the service. Since many of the technological features of cloud computing are entirely new, there are no long-term studies or broad experiences with the services. Buyers must therefore rely on information they receive from the media and base their decisions on incomplete facts.

Privacy laws

Furthermore, the results of this study indicate that the German privacy laws are influenced by the German cultures. This finding is in agreement with Lim et al. (2004, p. 547) who argued that people from cultures with high uncertainty avoidance levels such as Germany show “higher needs for structure (i.e. formal rules and regulations), and stronger faith in institutions (e.g. the government)”. These cultures “often attempt to minimize risk by following established rules and norms” (Dinev, Goo, Hu, & Nam, 2009, p. 7). Krasnova and Veltri (2011) pointed out that U.S. citizens would leave many privacy issues to industry self-regulation while Germans would rely on a

comprehensive legal framework for all aspects of personal data collection, access and use (R. Anderson, 2008; Bellman et al., 2004). According to Hofstede (2018), U.S. Americans are less emotionally expressive and require less rules than cultures with a higher uncertainty avoidance score. Krasnova and Veltri (2010) argued that societies with a higher uncertainty avoidance score typically have stricter laws to protect individuals. This confirms the assessment in Section 2.1.6, that Germany and the EU had a complex set of different regulations, policies and legal frameworks in place to protect the privacy of their citizens that reflect the public opinion about data privacy matters. The GDPR is the most recent example of the strict data privacy stance of Germany and the EU.

Additionally, Krasnova and Veltri (2010, p. 6) reasoned that countries with a higher level of uncertainty avoidance, such as Germany, are “associated with more pessimistic perspectives on the incentive of companies”. One of their findings was that whereas 29% of the U.S. participants agreed that Facebook was competent in protecting user information, only 7.3% of the German respondents shared that opinion (Krasnova & Veltri, 2010, p. 7). This might contribute to the fact that German Internet users prefer to use pseudonyms for their Facebook profiles (see Section 6.1.2.1). The difference in the uncertainty avoidance dimension and the assumption that the U.S. society requires less rules might also be an explanation why the U.S. economy is less regulated than the Germany market. For example, as some of the IT managers explained in the interviews, the German insurance sector is regulated by a dedicated supervisory authority that enforces strong restrictions on data storage and processing. This might lead to the situation that U.S. cloud provider sales organisations do not understand the individual challenges of German companies to move their IT to the cloud. The key informants in the current research also stated that Germans favour transparency and that cautiousness was part of the German culture. Krasnova and Veltri (2010) stated that, since the German culture has a higher degree of uncertainty avoidance, German Internet users may be more demanding in terms of transparency of data handling and processing and dissatisfied with providers that are vague about their processes and procedures.

Srite and Karahanna (2006) maintained that strong legal protections can have the opposite effect and, paradoxically, lead to a lower level of trust. Krasnova and Veltri

(2010, p. 6) found that the German respondents attributed higher probability to situations when their personal information becomes accessible to “unknown individuals or companies without their knowledge” than the U.S. participants. This is in contrast to the stricter privacy regulations in Germany. Krasnova and Veltri (2010, p. 6) explained this finding with the higher level of uncertainty avoidance in Germany which “often leads to anxiety and exaggerated fears” in combination with the foreign origin of U.S. social network service providers. This view was shared by both groups of respondents of the current research who stated that German companies see a high risk in storing their data at public cloud providers and that U.S. citizens were less worried about using public cloud services.

Technology adoption

According to the sellers from the U.S. cloud providers, other European countries such as the Scandinavian countries and the UK were embracing cloud services, while Germany and Austria were more conservative with adopting cloud technologies. However, the sellers also reported that German companies targeting an international market were more open for adopting cloud technologies. This is in line with the cloud adoption statistics discussed in Section 2.1.5. Moreover, the findings of the current study are consistent with those of Hofstede (2003a) who suggested that cultures with a high level of uncertainty avoidance such as Germany would be less open to the adoption of new innovations and technologies. The U.S., on the other hand, has a low score in the uncertainty avoidance dimension and, as a consequence, there is a high openness for new ideas and innovative products. This includes latest technologies and new business practices (Hofstede, 2018). Similarly, in their analysis on how user perceptions of privacy mediate the relationship between national cultural values and attitude towards using instant messaging, Cao and Everard (2008) found a strong positive link between uncertainty avoidance and using the technology. In another review on the influence of national culture on information technology adoption, Leidner and Kayworth (2006, p. 366) found that uncertainty avoidance was the “most used dimension” in nine out of ten studies that mentioned Hofstede’s cultural values to “describe the relationship between national culture and IT use and adoption”.

One of the core ideas of these studies was that uncertainty avoidance plays an influential role in how individuals and groups will adopt information technologies.

These studies reason that information technology is “inherently risky” and that cultures that avoid uncertainties are less likely to adopt and use any new technologies (Leidner & Kayworth, 2006, p. 366). For example, in a survey with businesses across 23 countries, Png, Tan, and Wee (2001, p. 36) concluded that “businesses from higher uncertainty avoidance countries were less likely to adopt frame relay” as a new technology. In a study with students from different countries, Thatcher, Stepina, Srite, and Liu (2003) found that participants from cultures with high uncertainty avoidance scores were less willing to try out new technologies. Previous studies on the impact of culture on the adoption of technology (e.g. from Hasan and Ditsa (1999), Sirkka L Jarvenpaa and Leidner (1998) and Straub, Keil, and Brenner (1997)) came to similar results.

The openness to technological innovation in the U.S. society might therefore be one of the reasons why U.S. cloud services are considered superior to German cloud offerings and why the respondents described U.S. cloud providers as the market leaders.

Trust building process

Krasnova and Veltri (2011, p. 893) speculated that cultures such as Germany with a high level of uncertainty avoidance are less likely to take a “leap of faith” and rather act on the basis of trust because they might be afraid of “becoming vulnerable to the other party in a transaction”. Likewise, Dinev et al. (2009, p. 5) argued that people in risk-averse cultures “attempt to control almost everything in order to avoid the unexpected”. On the other hand, cultures with low uncertainty avoidance, such as the U.S., may focus less on the privacy concerns but rather concentrate on evaluating the trustworthiness of the other party (Krasnova & Veltri, 2011). As argued by Doney et al. (1998, p. 614), trustors in low uncertainty avoidance cultures are “more likely to form trust via a calculative process” while trustors in high uncertainty avoidance cultures are “more likely to form trust via an intentionality process” or “via a prediction process”.

The U.S. as a low uncertainty avoidance culture is therefore establishing trust via a calculative process where trustors must determine whether the targets' costs for opportunistic behaviour exceed the benefits (Doney et al., 1998). Hence, trust is formed in a calculative process where each party calculates the rewards and costs of the other party cooperating or cheating (Lindskold, 1978). Germany, on the other

hand, as a high uncertainty avoidance culture, would therefore form trust via a prediction process or an intentionality process. Trust based on prediction depends on the ability of each party to forecast the behaviour of the other party (Deutsch, 1960). In this process, the trustor determines if the past actions of the other party provide a reasonable basis for predicting future behaviour (Good, 1988). Therefore, trust building through a prediction process entails information about a party's past actions. For example, in the case of public cloud services, German companies would study the past behaviour of cloud providers and other parties involved such as foreign governments to predict future risks and opportunities.

The intentionality process aims at determining the intentions of the other party by interpreting their words and behaviour (Lindskold, 1978). In case one party is perceived in having only selfish intentions it is unlikely that trust is built (Lindskold & Bennett, 1973). To establish trust via an intentionality process, the intentions of the other party must be perceived as benevolent (Larzelere & Huston, 1980; R. C. Mayer et al., 1995). As described by the IT managers of the German companies, it was difficult or impossible for them to tell if the U.S. cloud providers would tell the truth about their involvement in the global surveillance activities of the U.S. government agencies or not. Since the buyers could not be sure of the sellers' intentions it was probably difficult to establish trust between the parties. Doney et al. (1998) suggest that when both parties share the same values and norms, the probability for a trusting relationship is higher. For example, U.S. salespeople try to gain buyer's trust by demonstrating their expertise (Swan et al., 1985) which is probably an efficient strategy in individualist societies (Doney et al., 1998).

This might be a valid approach in individualist societies such as the U.S. where "people generally value evidence of individual initiative and achievement" (Doney et al., 1998, p. 616). On the other hand, a lack of similarity in cultural standards may result in a failure of the trust-building process. For example, collectivist societies might distrust salespeople who stress their individual accomplishments instead of referring to successful business in the past or accentuating the good intentions of the seller. These different approaches in the U.S. and Germany for establishing trust between buyers and sellers would emphasize the importance of local salespeople in Germany working for U.S. cloud providers. As argued by the sellers in the current research, German

companies would be more open to testing and purchasing U.S. public cloud services when they could talk to local experts in their native language. However, as reported in Section 5.10, the German buyers maintained that their purchasing decisions was not influenced by local salespeople and that they would make their decisions independent from the availability of a local salesforce. This conflict will be discussed in more detail in Section 6.2.3 on salesperson trust (RO2c).

6.1.2.3 Long-term orientation

The largest deviation between the two cultures can be found in the long-term orientation dimension which describes “how every society has to maintain some links with its own past while dealing with the challenges of the present and future”. As described above, Krasnova and Veltri (2011) referred to the scores defined by Hofstede (2003a) and not to the updated long-term orientation scores by Hofstede and Minkov (2010). Therefore, Krasnova and Veltri (2011) argued that both cultures, the U.S. and Germany, exhibit low long-term orientation. Consequently, Krasnova and Veltri (2011) focused on the dimensions of individualism and uncertainty avoidance instead. With a score of 83, Germany is considered as a pragmatic country. People in pragmatic societies believe that “truth depends very much on situation, context and time”. In general, they have a tendency to save and invest, thriftiness and persistence in achieving results (Hofstede, 2018).

As described by the IT managers in the interviews, German companies have invested in their own IT infrastructure in the past and the majority of the respondents planned to continue to invest in their private cloud infrastructure in their on-premise data centre instead of migrating to a public cloud. If the IT strategy of German companies is aiming for long-term solutions, a migration to the public cloud would require a systematic analysis of the benefits and risks, as well as a dedicated project, budget and timeline for the migration. This could be another reason why public cloud adoption in Germany is slower than in the U.S. or other countries.

The U.S. is rated as a normative society with a low score of 26. According to Hofstede (2018, p. 2), many U.S. citizens have very strong opinions about “what is good and evil”, e.g. in topics such as weapons, abortion and “the size and rights of the government versus the States and versus citizens”. As presented in the findings, the German IT managers gave similar examples in the interviews about their view of the

U.S. American culture. For example, one of the buyers expressed his incomprehension at the fact that a large number of U.S. citizens would be killed every year because of a wide distribution of firearms in the country. Other respondents puzzled the negative attitude of many U.S. citizens towards the introduction of a public health care system. A major criticism by the German IT manager was, however, the approach of the U.S. government for protecting the country by using mass surveillance tools. As explained by some of the buyers in the interviews, their contacts in the U.S. did not share their negative stance towards the surveillance activities of the U.S. government agencies but accepted the intrusion into the private sphere of foreign and U.S. citizens. The German buyers had the impression that U.S. citizens would not be worried about these activities as long as the justification was the protection of the American people against foreign attacks.

Additionally, U.S. companies are described as measuring their performance on short-term basis which drives company owners and employees to strive for quick results at work (Hofstede, 2018). The sales representatives of the U.S. cloud providers reported that their U.S. headquarters showed little understanding for the slow cloud computing adoption of German companies. They described that they had to meet their sales and deployment targets for the fiscal year and that it was up to them to achieve this goal. Moreover, Acquisti (2004) argued that cultures with a low score on long-term orientation may have stronger preferences for immediate benefits and hence be less afraid about privacy despite possible negative consequences in the future. The statements of the respondents of the current research that U.S. citizens are less worried about their data privacy support this presumption.

6.1.2.4 Indulgence

The indulgence dimension is the latest addition to the cultural dimensions of Hofstede (2018, p. 3) and is defined as “the extent to which people try to control their desires and impulses”. Germany has an indulgence score of 40 which, according to Hofstede (2018), indicates that the German culture is restrained in nature. Those societies are described as having a tendency to pessimism and cynicism. Additionally, restrained societies have more control over their desires and put less emphasis on leisure time.

It could be argued that the IT managers of the German companies painted a gloomy picture about the risks and future of public cloud computing and that their expectations

of the future development of cloud computing usage in Germany was rather pessimistic. For example, some buyers stated that they would prefer to avoid all U.S. technology products if they could. As expressed by some cloud sellers, the reactions of the German companies on their trust in public cloud services were oftentimes rather emotional and strongly influenced by the surveillance scandals. The local sales representatives of the U.S. cloud providers described the German people as negative, cautious, sceptical and conservative and gave the example that Germans would even publicly protest against population census activities. Hence, the already pessimistic view on the risks and benefits of public cloud computing of the German IT decisions makers could have potentially been reinforced by the Snowden revelations.

Additionally, the respondents mentioned that German engineers prefer to build their own technical solution over buying or adopting products or services from other countries. The cloud sellers reported that German companies had more trust in what they called German engineering and would choose their own or local products over foreign solutions. They further commented that American engineers would focus on being innovative whereas Germans would focus on the potential downsides. Moreover, Germans would be unwilling to acknowledge that Americans are better in something and would believe that they could do it better themselves. This assessment is shared in the practitioner literature about cloud computing. Germany is seen as the “country of engineers” which means technical solutions need to be fully developed and matured (Mauerer, 2016). The circumstance that most of the buyers prefers to run their IT in their own data centres affirms this stance (see Section 5.8).

The U.S., on the other hand, is described as showing a contradictory behaviour with a “work hard and play hard” attitude. Hofstede (2018) calls the U.S. as a “prudish” society where even moral evangelists may appear to be immoral. Hofstede gives the example that “drug addiction in the States is higher than in many other wealthy countries” although the U.S. government “has waged a war against drugs and is still very busy in doing so”. The examples given by the buyers support the argument that some aspects of the U.S. culture appear contradictory from the point of view of German citizens. These examples included the wide distribution of firearms in the U.S. and the discussions around public healthcare as discussed above.

Further research regarding the role of national culture on the trust relationship between these groups would be worthwhile. The current research discussed the characteristics of the U.S. and German culture based on Hofstede's cultural dimensions and found several peculiarities of the German and U.S. culture that could contribute to the relatively low adoption of U.S. cloud services by German companies. However, if the debate is to be moved forward, a better understanding of the cultural factors that have an influence on the trust between German buyers and U.S. sellers needs to be developed. Especially the issue of culture and foreign government trust is an intriguing one which could be usefully explored in further research. Moreover, from a practitioner perspective, it would be interesting to assess the effects of actions that can build trust between businesses with different cultural backgrounds.

In addition to Hofstede's cultural dimensions, two additional aspects, history and age, had probably an impact on the trust of German companies in U.S. cloud providers. As argued by the respondents, the culture of a country is shaped by its history. However, cultural characteristics of a society might develop and change between generations.

6.1.2.5 History

As reported by the buyers in the current research, Germans tend to be more restrictive regarding to data privacy. This might, however, in the case of Germany be reinforced by the history of the country. The key informants of the current study argued that the German culture, particularly in terms of data privacy matters, was strongly influenced by its history. They further reasoned that U.S. citizens could not understand their position since they did not share the same history with the Nazi Secret State Police (GeStaPo) and the State Security of the GDR (StaSi) and did not experience national security agencies spying on their own citizens. Likewise, the cloud sellers maintained that the culture of a country is shaped by its history and that the Germany history was particularly influential regarding privacy sensitivity. According to the sellers, some senior managers of their customers might have witnessed the surveillance activities of the StaSi themselves if they lived in the GDR before.

The findings of the current study are consistent with those of Krasnova and Veltri (2010) who found that their German respondents perceived more damage of the disclosure of their private information to government agencies than the U.S. participants. They argued that this could be explained by the fact that "government

oversight was a big concern in not too distant past during the oppressive Nazi regime and then subsequently in East Germany" (Krasnova & Veltri, 2010, p. 6). For example, the former East Germany had "some 25,000 telephone taps in place, despite having a fraction of the U.S. population" (R. Anderson, 2008, p. 778). Lichter, Löffler, and Siegloch (2016, p. 1) studied the long-term consequences of government surveillance in Socialist East Germany and concluded that the surveillance activities led to "lower levels of trust and reduced social activity in post-reunification Germany" and long-lasting negative economic effects such as higher unemployment and larger out-migration. The authors showed that these effects were due to surveillance and not alternative mechanisms and argued that their findings have important implications for contemporary surveillance systems such as the global surveillance activities of the U.S. government agencies. Lichter et al. (2016, p. 4) referred to Schneier (2013) and G. Gao (2015) and stated that "the revelation of the NSA secrets affected ordinary peoples' trust in the government" and that "a substantial share of people stated that they adjusted their use of telecommunication as a consequence of the Snowden affair". Hence, the global surveillance activities could not only have negative effects for the U.S. cloud providers but for the U.S. economy in general.

As stated in Section 2.1.5.1, U.S. President Barack Obama and many others also argued that the German history was one of the reasons why Germany was particularly sensitive about data privacy matters. The fact that both groups of respondents, buyers and sellers, brought up the idea that the German history had an impact on the present cloud adoption issues can be interpreted as a strong indicator for the importance of the cultural background for the trust of German companies in U.S. cloud services.

6.1.2.6 Age

Another finding was that both buyers and sellers shared the opinion that younger people are, on average, more open towards modern technologies and cloud services and that this might be a generational issue. According to the respondents, this would also apply to younger IT decision makers.

However, studies focusing on the privacy concerns among young people and adults offer contradictory results. A research conducted by Moscardelli and Divine (2007) found that adolescents are less worried about data privacy when using Internet services than adults. Additionally, young people who grew up with the Internet tend to

use more online services than older people (Lenhart & Madden, 2007a). This is especially the case with so called “digital natives” who grew up with the Internet (Palfrey & Gasser, 2011). A more recent study from Sweden came to a similar result and showed that adult Internet users took slightly more care of their online privacy than younger people (Rodriguez & Obradovac, 2017). Furthermore, an online survey with 18- to 65-year-old Dutch-speaking adults revealed that respondents in young and middle adulthood were more vulnerable in terms of privacy protection than emerging adults (Van den Broeck, Poels, & Walrave, 2015).

Other studies, however, found that young people were more concerned about their privacy than adults. For example, Caverlee and Webb (2008) found that young Internet users were more likely to create private user profiles to protect their privacy than older users. The authors assumed that the younger people had more knowledge about Internet technologies and would therefore be able to protect themselves in better ways. Likewise, Lenhart and Madden (2007a) concluded that teenage social media users were more cautious than adult users in protecting their online privacy and that the likelihood of sharing personal information on social network sites increased with age (Lenhart & Madden, 2007b). Blank, Bolsover, and Dubois (2014) also reported that young Internet users were actually more likely to protect their online privacy than older people. In their literature review on youth and online privacy, Marwick, Murgia-Diaz, and Palfrey (2010) concluded that, although privacy settings on social network sites are often difficult and confusing, most young people restrict access to their online profiles.

A third group of studies found no significant variance between the age groups. In a study conducted by Hoofnagle, King, Li, and Turow (2010, p. 2), the privacy attitudes of young U.S. adults did not differ from those of older adults and the authors concluded that “young-adult Americans have an aspiration for increased privacy even while they participate in an online reality that is optimized to increase their revelation of personal data”. Steve Jones, Johnson-Yale, Millermaier, and Perez (2009) argued that young people would differentiate between social network services and other (confidential) information. They found that about three quarters of college students would be concerned about the security of their passwords and credit card numbers but not about the information they were sharing on social networking sites.

Miltgen and Peyrat-Guillard (2014, p. 116) tried to investigate some of the contradictions and paradoxes in previous literature and concluded that the “reversed privacy paradox” of young people could be explained with a combination of lower privacy concerns and a greater use of protection strategies. The authors claimed that younger people (age 19-24) would feel more positive, more responsible and more confident of their ability to prevent a misuse of their data whereas middle-aged people (age 45-60) perceived higher risks and had more negative views about data use and disclosure. Younger adults (age 25-44) took an intermediate position and were neither confident nor untrusting. These results confirm the findings of Moscardelli and Liston-Heyes (2004) and Palfrey and Gasser (2011) that young people show less privacy concerns than adults. Additionally, Miltgen and Peyrat-Guillard (2014) supported the findings of Lenhart and Madden (2007b) and Moscardelli and Divine (2007) that young people use pseudonyms and post fake information to protect their identity whereas adults provided real personal information.

However, parents may be able to have a strong influence on their children’s online privacy. According to Youn (2009), young Internet users tend to protect themselves if they see themselves as vulnerable and perceive privacy risks. The results of the study by Moscardelli and Divine (2007, p. 232) “suggest that heightening adolescents’ concern for their privacy will lead to a greater likelihood that they will use a number of different privacy-protecting behaviours”. Another study by Steeves and Webster (2008) proposes that parental supervision can reduce privacy risks of young people with social network site use. From a gender perspective, men are probably less worried about data privacy than women. Fogel and Nehmad (2009) found that women have greater privacy and identity information disclosure concerns than men. A more recent study by J. T. Child and Starcher (2016, p. 1) confirmed that men “enacted significantly less Facebook privacy management than did women”.

The comments of the interviewees of the current research hint at a change in the perception of modern technologies and privacy threats over generations in the German society which could have an impact on cloud adoption rates. However, since the current research and the interview questions did not focus on the impact of the age of Internet or public cloud services users on trust and data privacy matters, there are only a few instances where interviewees commented on the age as an influencing

factor. The studies cited above mostly focused on consumer trust and privacy concerns and not on the perspective of business customers. Additionally, the focus was mainly on e-commerce websites and social network sites and not on storing company data with public cloud services. Hence additional research is required to analyse the impact of the age of a public cloud service buyer on the trust and privacy concerns he or she has with respect to public cloud services.

In future investigations, it might be possible to use a different approach in which the cultural differences are studied over a longer period. As argued by Wright and Ehnert (2010, p. 123), cross-cultural trusting encounters are likely to involve actors such as the U.S. cloud sellers and the German IT managers who, at different times during this interaction, “are being oriented in their actions by complex combinations of contextual forces”. The authors maintained that longitudinal research was sensitive to these temporal changes that it was an important part of producing rich descriptions of cross-cultural trusting to include these time-based perspectives. Therefore, a longitudinal study could offer the opportunity to learn about the different stages and dependencies in the trust formation process. Additionally, given that the current research focused specifically on the time shortly after the global surveillance disclosures, a longitudinal assessment would also extend the findings with regard to the growing cloud adoption in Germany. This extension is important because the number of German companies adopting public cloud computing services is constantly growing and it would therefore be interesting to understand if and how the views of the buyers and sellers changed over time.

6.1.3 Influence of the sector (RO1c)

The findings provided important insights into the influence of the sector of a business as well as the size of a company on the adoption of public cloud solutions from U.S. cloud providers. As described in the previous chapter, the current research presumed that the sector of a German company would not have a noteworthy influence on the cloud adoption rate. However, the answers of the interviewees suggest that the sector played a substantial role. It can therefore be concluded that the original assumption made in Section 2.1.5 regarding the role of the sector was wrong and that future research should take the impact of the sector into account.

The original assumption made in Section 2.1.5 was based on a study conducted by Techconsult (2012). However, a subsequent study by KPMG (2014, p. 9) reported that there was a difference in cloud adoption between sectors but that these "differences between sectors and industries became smaller" over the last years. The only exception was the IT and telecommunications sector with 60% of "open-minded and interested" people, which was excluded from the current research (see Section 2.1.5). A more recent survey from KPMG (2016) shows that there is still considerable difference in cloud adoption between sectors in the German market (see Figure 16). Interestingly, the banking industry, which is considered a highly regulated sector in Germany, had one of the highest cloud adoption rates in the KPMG (2016) study. This is, however, in contrast to the findings of the current research, where the respondents argued that banking and insurance institutes are subject to strict compliance requirements regarding public cloud services.

It is difficult to explain this result, but it might be related to the different years in which the surveys have been conducted. Another possible explanation for this inconsistency is that it was not clearly defined if private cloud implementations are included and to what extend those companies have migrated IT services to the cloud.

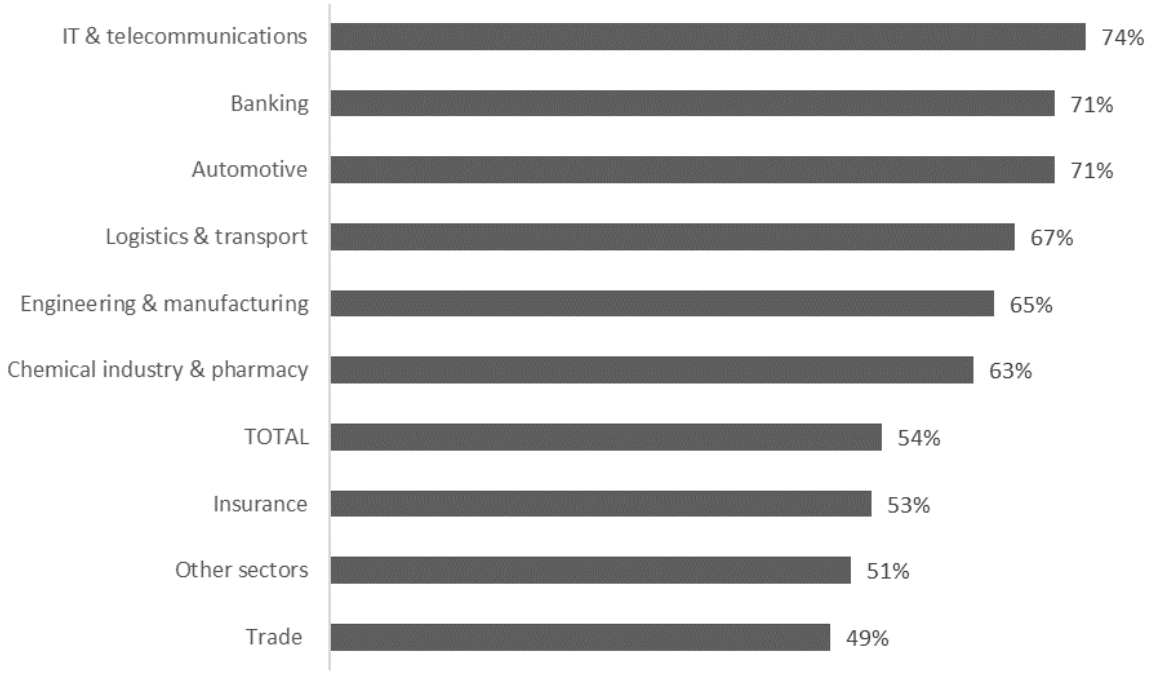


Figure 16: Cloud usage by sector. Adapted from KPMG (2016).

The key informants for the current study came from nine different sectors. Although the total number of respondents for each sector (between one and two) cannot be representative, it might be helpful to get a consolidated view on the differences experienced in the current research. Table 24 gives an overview of the sector-specific views on the legal constraints for adopting public cloud services, the fears of shadow IT and economic espionage, and the need for a local sales representative.

Table 24: Properties of sectors included in the current research

Sector	Respondent	Legal constraints	Afraid of shadow IT	Afraid of economic espionage	Need local salesperson
Insurance	Buyer01 Buyer07	Yes	Yes	Somewhat	Somewhat
Advertising	Buyer02	No	No	No	No
Conglomerate	Buyer03	No	Yes	Yes	No
Manufacturing	Buyer04	No	Yes	Yes	No
Electric utility	Buyer05	No	Yes	No	Somewhat
Banking	Buyer06	Yes	Yes	Somewhat	Yes
Industrial equipment	Buyer08	No	Yes	Yes	Yes
Entertainment	Buyer09	No	No	No	Somewhat
Logistics	Buyer10 Buyer11	No	Yes	Somewhat	Somewhat

The following sections will discuss these differences by reference to the statements of the respondents and the literature.

Legal constraints

As described in the previous chapter, the financial services sector is subject to certain regulatory constraints which make it difficult for insurance companies and banks to store their data in public cloud data centres and even more challenging if these data centres are operated by foreign companies. As described by Guenzi and Georges (2010, p. 117), the financial services sector is characterised by “technical complexity, information asymmetry and long-term return on investment” and “all these factors emphasize the importance of trust in the financial services industry”. The respondents explained that the German insurance sector was subject to specific regulatory requirements which they had to be compliant with.

One of these legal provisions was the German Criminal Code Section 203 “violation of private secrets” which states that private health, accident or life insurance companies are liable to imprisonment or a fine for disclosing secrets of their customers (Germany, 1998). Furthermore, they stated that insurance companies were subject to the critical infrastructure protection programme coordinated by the German Federal Ministry of the Interior (Germany, 2011). This means that every attack on the infrastructure of a public cloud provider would have to be reported to the German government, which was not feasible from the point of view of the interviewed companies. However, Adjei (2015, p. 64) found that trust was the main barrier “for cloud computing service acquisition by financial institutions”. Participants from other sectors, however, did not mention any legal restrictions for storing their data in a public cloud environment.

Shadow IT

Most of the sectors included in the current research had policies against non-official IT in place. These companies identified shadow IT as a major threat to their IT security and did not tolerate non-official cloud services.

However, more agile and open businesses such as the advertising and entertainment industries were less afraid of the existence of shadow IT cloud services. Moreover, IT services that were not officially provided by the IT departments were in some cases part of the overall corporate strategy. The respondents from the media and entertainment industries argued that the risk for using cloud computing services was comparably low in relation to other industries. The phenomenon of shadow IT will be discussed in more detail in Section 6.2.1.3.

Economic espionage

The fear of economic espionage was one of the key reasons why sectors like automotive and manufacturing industries were particularly cautious about storing their data with U.S. cloud providers. In comparison, the manufacturing and industrial equipment industries are most worried about intellectual property theft whereas the advertising and entertaining companies did not worry about this possibility. Since these companies are dependent on their technological lead in a certain field, the risk of losing company secrets to the competition outweighs the potential benefits they see

from migrating this data to the cloud. Consequently, cloud providers need to actively address this fear and develop a concept that convinces companies that are afraid of economic espionage to trust public cloud computing providers with their most valuable data.

Other sectors such as insurance, banking and logistics were somewhere in between these positions and recognised economic espionage as a potential danger which needed to be taken into consideration. This topic will be discussed in more detail in Section 6.2.4.2.

Local sales representatives

A local sales representative of a public cloud provider was important to the banking and industrial equipment sector, somewhat important to the insurance, electric utility, entertainment and logistics sector, and not important to the advertising, conglomerate and manufacturing firms.

However, Section 6.2.3 will argue that the statements of the key informants regarding their need for a local sales representative are inconsistent and contradictory. This might explain why there is no clear pattern of similar industries such as insurance and banking or manufacturing and industrial equipment regarding their preference for local sales support.

Further data is required to determine exactly how the trust differs between different sectors in Germany. For instance, the manufacturing industry might be particularly afraid of economic espionage and other sectors might have other concerns that were not identified in the current research. Due to the scope of this research, the current study was unable to analyse these variables in more detail.

Size

Another finding was that the size of a company was mentioned as an additional factor influencing the decision regarding public cloud adoption. From the perspectives of several buyers and sellers, larger companies were less concerned about storing data in public cloud services than small and medium businesses. According to the respondents, this was particularly the case for companies that also operated outside of Germany. This is consistent with surveys about public cloud adoptions of SMEs in Germany presented in Section 2.1.5. For example, a survey conducted by KPMG

(2014) showed that cloud adoption was much higher for large enterprises with 2,000 or more employees and that small firms with 20 to 99 employees were much more undecided or critical. Hayes (2008) and Low, Chen, and Wu (2011) found that large enterprises, due to more resources and a greater ability to take on risks, have a higher probability of adopting public cloud computing services. Small companies, on the other hand, need to trust their providers “for reliable delivery of quality products” in order to stay competitive (Chow & Holden, 1997, p. 295). This gap is, however, closing. A more recent study of KPMG (2017a) showed that SMEs were in 2016 almost on the same level as larger companies with 2,000 or more employees.

Nevertheless, according to the sellers, start-up companies were mostly open to cloud computing technologies and a number of start-up companies based their business model on public cloud services. The cloud sellers argued that cloud services were often part of their business model and that they were not able or willing to invest in their own server hardware and IT staff. This is in line with the business benefits of public cloud computing described in Section 2.1.3 where it was argued that start-up companies have the ability to create business models that have not been possible in the past (R. Smith, 2009; Wang et al., 2017). Start-ups can just rent the necessary computing, storage and communication capacities from cloud providers and only pay for the volume of the services that they actually use (Wang et al., 2017). This lowers entry barriers into existing and new markets and makes start-up companies a popular target for public cloud providers (CEBR, 2011; Wang et al., 2017).

Since the current research focused on large German companies, the question arises how the findings of the current research are representative for the entire German economy, including SMEs. The fact that German SMEs are even more reluctant to adopting public cloud services than large German enterprises suggests that the lack of trust and fears regarding data privacy and economic espionage are even stronger at SMEs than at large companies. However, since SMEs account for the majority of companies in Germany it would be interesting to assess the effects of the company size on the importance of the trust relationships and how U.S. cloud providers can win the trust of SMEs. It is therefore likely that the average German company has less trust in U.S. public cloud services than the respondents of the current research. Consequently, U.S. cloud providers need to be aware that they could face strong

resistance from German SMEs regarding public cloud adoption. Further research needs to examine more closely the links between company size and trust in U.S. public cloud services.

Further research could also be done to investigate if the findings of the current study are applicable to companies (buyers) from other countries or to cloud providers (sellers) that are not registered in the U.S. As explained above, this decision was based on access to key informants in Germany and the fact that the cloud solutions from U.S. companies are considered the worldwide market leader. Another consideration for the selection of these two markets were the reports on the surveillance activities and the reactions from German companies to the disclosures. The reactions to the global surveillance disclosures and the trust in U.S. cloud providers may differ in other European countries or countries outside the EU. Furthermore, the answers of the key informants of the German companies might have been different if the cloud provider was registered in an EU country such as Austria or in a country outside the EU such as Canada, Brazil or China. By exploring the concept of trust in different countries, a more global approach to B2B marketing and the impact of trust could be incorporated into strategic planning for international organisations.

6.1.4 Summary

This research confirms current knowledge about the importance of trust for social life and business relationships studied by philosophers, sociologists and economists. Moreover, the current research found that trust is also a key factor for public cloud computing adoption. Therefore, the findings of this study suggest that selling companies should proactively invest in building up a trustful relationship with their clients and recruit and train their staff accordingly.

The trust between buyers and sellers is highly influenced by their cultural background which is in line with previous research. For example, the general thoughtfulness regarding the protection of personal data and company data had the consequence that German companies reacted stronger to the revelations of the global surveillance activities than other countries in the EU or other parts of the world. Other aspects of the German culture such as “German Angst”, general cautiousness, resistance to change, unwillingness to take risks and perfectionism also have an impact on the trust relationship between German companies and U.S. cloud providers.

An unexpected finding was the influence of the sector or size a company is operating in on the adoption of public cloud services. Current studies presented conflicting outcomes of the relationship between sector and cloud adoption. Early studies found no impact of the sector on public cloud usage while more recent surveys came to the conclusion that certain industries were more open to adopting cloud services. However, the current research identified different sectors as hesitant to cloud usage than previous studies. This relationship between the buyer's sector and the willingness to adopt public cloud solutions should be investigated in more detail in future research.

6.2 Trust relationships (RO2)

The second main objective of this research was to explore the trust relationship between German companies and U.S. cloud products (RO2a), U.S. cloud provider companies (RO2b), the local sales representatives of the U.S. cloud providers (RO2c) and the U.S. government (RO2d). The following section will focus on the first of these four trust relationships by discussing the findings regarding the trust of the buyer (represented by the key informants of the German companies) in the product (in form of the U.S. cloud computing services).

6.2.1 Product trust (RO2a)

The first theme that will be discussed is the attitude of the German companies towards cloud computing technologies in general. This is followed by a discussion on the capabilities of U.S. cloud services in comparison to products from German or European companies. The last part addresses the implications of shadow IT cloud services in German companies.

6.2.1.1 Cloud computing technology

The findings suggest that the cloud technology itself was not the reason why the adoption of public cloud services by German companies was relatively low. Although cloud computing technology involves certain risks such as availability, reliability, performance and data security issues (see Section 2.1.6), it appears that these risks can be proactively managed by the cloud consumers. It can therefore be argued that a substantial proportion of the German companies had trust in the product, the cloud computing service, as defined by Plank et al. (1999, p. 62), in the way that it fulfils "its functions as understood by the buyer", such as reliability and performance.

Lansing and Sunyaev (2016, p. 70) created the term “trust in cloud ecosystem” which they defined as the believe “that the nested network of providers in the cloud computing ecosystem is capable of providing an infrastructure that allows sourcing of cloud services according to one’s confident expectations”. The authors concluded that “trust in cloud ecosystem leads to trusting beliefs in provider and trusting beliefs in IT” (Lansing & Sunyaev, 2016, p. 78). The buyers cited several business advantages of public cloud computing services such as shorter time to market, flexibility and cost savings. This is, however, in contrast to the decisions of German companies to avoid public cloud providers and keep their IT in their own on-premise data centres (see Section 6.2.2.3).

Intangible goods

In contrast to selling tangible goods, service selling mostly involves long-term commitment and “a continual stream of interaction between buyer and seller” (Crosby et al., 1990, p. 68). As explained in Section 2.1, cloud computing includes a growing list of technology services that are constantly evolving and changing and require sellers and buyers to keep up with these changes. It could therefore be argued that a close relationship with a sales representative and/or technology consultant of the selling company would be beneficial for the buyer to keep track of developments and take informed decisions. Similarly, Chow and Holden (1997) argued that long-term relationships may be most difficult to services because buyers might be rather intolerant of any sign of inadequacy on the part of the seller upon whom they depend. The authors concluded that the level of trust and cooperation, as well as the adaptation to uncertainty moderate the degree of the success of the long-term relationship. Likewise, Palmatier et al. (2006), argued that services are perceived as less tangible than physical products and this may make the characteristics of trust more critical because assessments can often be ambiguous. The authors concluded that the role of trust may take an added importance in developing long-term relationships in a services context.

Doney, Barry, and Abratt (2007) studied trust in global B2B services and recommended that services providers should invest in both economic and social aspects of the transaction. The authors found that “buyers expressed considerable frustration as to the service provider’s lack of customer orientation” and that they were

“clueless as to the buyer’s mission tensions” (Doney et al., 2007, p. 1110). This supports the findings of the current research that German companies were looking for service providers who would understand their business and that customer orientation is an important antecedent of trust. According to the buyers, their internal IT departments would understand their business model well and would support the business departments with adequate technology solutions. Doney et al. (2007, p. 1110) recommended that salespeople should be trained to “recognize the intangible facets of relationship marketing” and contact their customers often. Moreover, according to the authors, sales managers should compensate their salesforce based on trust-building behaviour and competitiveness of the service offering.

6.2.1.2 U.S. cloud services

The findings support the assessment in Section 2.1.4, that the most advanced public cloud computing solutions are offered by U.S. cloud providers. As maintained by several market research organisations and analysts, the public cloud computing market in Europe is dominated by U.S. cloud providers (Büst, 2016; Castro, 2013; Experton, 2012; Herrmann, 2017; Millard, 2013; Schechner, 2016). As illustrated by the European Commission (2015b), nine out of the top ten cloud providers in the European market are headquartered in the U.S. with SAP as the only European provider. The respondents mentioned several reasons for the dominance of U.S. cloud service providers that were also described in Section 2.1.4 such as the size of the U.S. domestic market and economies of scale (European Commission, 2015b), a first-mover advantage (TNW, 2016), the availability of skilled staff (Experton, 2012) and legal constraints (European Commission, 2015b).

It can therefore be argued that a lack of functionalities in U.S. cloud services was not a reason why German companies would avoid U.S. cloud providers. Moreover, if German companies would focus on the functionalities and price to get the most business benefits from their cloud computing investments, they should consequently select U.S. cloud providers. Hence there should be other reasons for the relatively slow cloud adoption of German companies.

Product quality

In case of the current research there was no negative feedback on the quality of the services provided by the U.S. cloud providers. According to the buyers, the U.S. cloud providers were several years ahead with regards to cloud technology in comparison to European providers.

In a study conducted by Kennedy et al. (2001, p. 81), “product quality was found to be the strongest indicator of ownership satisfaction, not service quality, ethical concern of the manufacturer or salesperson characteristics”. Additionally, product quality did not have any influence on the trust of the salesperson (Kennedy et al., 2001). However, the salespeople in the study of Kennedy et al. (2001) were not employed by the manufacturer which might have an impact on this result. Likewise, Gounaris (2005, p. 18) found that “the degree of trust between the service provider and the customer is directly influenced by the quality of the service”.

Hence, the quality of the services offered by the U.S. cloud providers was probably not a reason why the German companies would distrust the providers.

Brand trust

According to the buyers, the U.S. cloud providers had a strong brand in the industry. Chaudhuri and Holbrook (2001) found that brand trust and brand affect were both directly related to purchase and attitudinal loyalty. Likewise, Delgado-Ballester and Luis Munuera-Alemán (2001) reported that brand trust was a key variable that generates buyer commitment and increases price tolerance.

However, the brand might rather be associated with product features and performance rather than trust in data privacy matters. Delgado-Ballester and Luis Munuera-Alemán (2001, p. 1254) recommended that companies should give the customer the perception that his/her “interests and welfare are considered by the brand” through honest communication and shared values to make the customer “feel secure and therefore trust the brand to meet his/her future satisfaction, even in new situations not previously experienced”. Conversely, when the actions of companies differ from the values communicated to them or when companies show unethical behaviour, brand trust may decrease (Portal, Abratt, & Bendixen, 2018). U.S. cloud providers might therefore want to focus their marketing initiatives on improving the trust of their

customers in their brand by giving their potential buyers the feeling that their data is secure and protected in a U.S. cloud service.

6.2.1.3 Shadow IT

Shadow IT can include all hardware, software and IT services that have not received any formal approval by the company's IT department but is used by employees of the organisation (Behrens, 2009; György, Cleven, Uebernickel, & Brenner, 2012). According to D'Arcy (2011), the consumerisation of IT and the rise of consumer cloud services brings shadow IT systems and new security risks to the IT department and the overall organisation. These risks could include increased risk for data leaks and loss (Shaikh, 2018), inconsistent workflows, wasted time and compliance issues (Walterbusch, Fietz, & Teuteberg, 2017). Other authors argued that shadow IT can compromise organisational data flows (D. Oliver & Romm, 2002) and undermine the official corporate IT systems (Strong & Volkoff, 2004).

According to the statements of the buyers and sellers of the current research, most of the German companies are already knowingly or unknowingly using public cloud computing services from unofficial sources. This confirms previous research where "all interviewees confirmed that their employees are steadily switching to mobile shadow IT, citing most of the time cloud services as the best example" (Silic & Back, 2014, p. 9). According to Silic and Back (2014, p. 2), "shadow IT is a currently misunderstood and relatively unexplored phenomena". The authors claim that shadow IT has an "important dual-use context" where its use can have positive and negative consequences (Silic & Back, 2014, p. 4). On the one hand, as described above, there is the possibility that shadow IT damages company data and undermines official systems. On the other hand, shadow IT systems can increase productivity by complementing existing standard systems (Behrens, 2009; Francisco, Jack, Joana, & Juan, 2017; Harley, Wright, Hall, & Dery, 2006). In general, corporate IT systems should be an enabler for business outcomes and align with the corporate business strategy (Henderson & Venkatraman, 1999; Luftman & Kempaiah, 2007). The lack of this alignment between business and IT may result in the creation of shadow IT systems (Silic & Back, 2014). For example, personal social media software services were used for improving internal business communication (D. Jones, Behrens, Jamieson, & Tansley, 2004).

However, as argued by Fürstenau, Rothe, and Sandner (2017), IT organisations might not be able to stop the spreading of shadow IT if they fail to address the underlying causes in terms of the requirements of the employees. As long as public cloud services offer productivity tools than the internal IT organisations are able to provide there is the risk of shadow IT services. Silic and Back (2014) even claimed that it was “very evident that there is a trust paradox where employees do not appear to trust their IT department”. In this case the corporate IT users might have more trust in the cloud services provided by external providers than in the offerings of their own IT organisation.

Yet, the U.S. cloud providers could benefit from this trend. As reported by some of the cloud sellers, they could use the fact that their German customers were already using public cloud services as a reasoning why these companies should consider U.S. cloud services. Nevertheless, while most traditional businesses tried to stop shadow IT to avoid data leakages, a few companies, e.g. in the media industry, embraced the diversity and flexibility of shadow IT. This is another example for the proposition that the openness of German companies regarding cloud computing technologies is strongly influenced by the sector they are operating in.

Overall, these findings indicate that there was a wish or need from the employees of the German companies to use cloud services that provide functionalities which they did not get from their own corporate IT departments. Moreover, German companies that claimed that they would not want to use public cloud services from U.S. providers were in some cases already using these services without their knowledge or permission.

6.2.1.4 Summary

All three themes discussed regarding product trust suggested that German companies had trust in the cloud technology and that a lack of product trust was not a determining reason why the adoption of public cloud services in Germany was comparably low. As argued above, the cloud service fulfils its functions as understood by the buyer, such as reliability and performance, and was therefore probably not slowing down cloud usage by German firms.

The second major finding confirmed the practitioner literature that the most advanced public cloud computing solutions were offered by U.S. cloud providers. The circumstance that U.S. cloud services were seen as superior to German or EU offerings indicated that a lack of functionalities in U.S. cloud services was no reason for German companies not to use public cloud services from U.S. providers either. In fact, if product features were the deciding factor, German companies should more likely purchase cloud services from U.S. companies than from German or EU providers.

The third finding demonstrated that there was a demand from inside the business departments of the German companies for cloud services. Both the buyers and the sellers reported that employees in German companies were using non-official public cloud services which can be categorised as shadow IT. The findings of the current research are in accordance with previous studies that found that shadow IT services are a widespread phenomenon and considered as unsafe by IT departments. It can therefore be concluded that the employees of German companies had a demand for public cloud services which contrasts with a low adoption of public cloud services by their IT departments.

In summary, it was unlikely that product trust was a key reason for the comparably low public cloud services adoption by German companies and it can therefore be concluded that there must be other explanations for this phenomenon.

6.2.2 Company trust (RO2b)

Research objective 2b is to explore the inter-organisational trust relationship between German companies and U.S. cloud provider companies. As defined in the literature review chapter, inter-organisational trust is the trust between the buyer and the selling company, which differs from the trust in the salesperson of the selling company (J. C. Anderson & Narus, 1990; Doney & Cannon, 1997; Dwyer et al., 1987; Ganesan & Hess, 1997). Salesperson trust, the trust of the buyer in the local salesperson of the U.S. cloud provider, will be discussed in Section 6.2.3 below. This section will focus on the inter-organizational trust, which A. Zaheer et al. (1998, p. 142) defined as the extent of trust placed in the partner organization (in this case the U.S. cloud providers) by the members of a focal organization (represented by the buyer of the German company). A. Zaheer et al. (1998) found that, in comparison with inter-personal

(salesperson) trust, inter-organizational trust was the dominant influence on performance and argued that companies should recognize the impersonal processes, structures and procedures that create a stable relationship. They gave the example of a purchasing manager who explained that the positive relationship with their business partner would continue when he would leave the company since both parties have been doing business together for many years. Likewise, Rutherford (2007) concluded that the relationship between buyers and the selling company is a stronger predictor of continuance than the relationship between the buyer and the salesperson. Moreover, for example in case of a conflict, salespeople can have a direct negative impact on the trust relationship between the buyer and the selling company (Rutherford, 2007).

Three central themes regarding the trust of German companies in U.S. cloud provider companies will be discussed in the next sections. The first theme is about the potential involvement of the U.S. cloud providers in the NSA surveillance activities and the consequences for the trust relationship with their German customers. The second section will discuss the reactions of German cloud providers to the NSA surveillance scandal and the trust of German companies in German cloud providers. The third and last topic is about the perspective of German companies towards private cloud or classic on-premise data centre solutions and how they compete with public cloud offerings.

6.2.2.1 U.S. cloud providers

One of the key findings regarding the trust of the German buyers in the selling company in form of the U.S. cloud provider was that even if most of the respondents believed that the U.S. cloud providers were not directly involved in the global surveillance programmes, they could not trust the cloud providers with their data. It could therefore be argued that the global surveillance disclosures led to a sustained reputational damage to the U.S. cloud providers.

Ethical behaviour

Although the U.S. cloud providers might not have been actively involved in the surveillance activities, it might be difficult for the U.S. cloud providers to convince the German companies that they were not involved in any criminal or unethical behaviour.

Kennedy et al. (2001) found that the perceived ethical concerns of a selling company played an important role in creating trust of both the salesperson and the selling company. The authors argued that business ethics not only had a positive impact on customer satisfaction and trust but also on business success and profitability. Likewise, Lagace et al. (1991) recommended that selling companies should create an environment where ethical behaviour is encouraged. As suggested by Moorman et al. (1993), organizational trust increases when salespeople and the selling company do not sacrifice ethical standards for business performance and profit goals. Ethical behaviour in sales can have important performance implications since ethical sales organisations are more desirable to work for and selling companies can increase their business with customers who demonstrate a desire to engage in ethical relationships (Evans et al., 2012). Being honest and "stand for what has been said and to point out if something is wrong" can lead to increased trust between buyers and sellers (Gustafsson & Folmerz, 2015, p. 61). According to Bateman and Valentine (2015), managers play a vital role in fostering an ethical climate and ethical sales processes and salespeople would observe the behaviour of their managers and peers carefully. Therefore, ethical behaviour of the selling company and the salesperson can have consequences for the trust of the buyer and the business performance.

In case of the global surveillance disclosures, it could be beneficial for the U.S. cloud sellers if they could convince the German buyers that they did not cooperate with the U.S. intelligence agencies and that their ethical standards would not allow to give customer data to third parties. However, this might be difficult to prove for the U.S. cloud providers which would in turn make it difficult for the German companies to trust them. According to the buyers, the U.S. cloud providers are subject to the U.S. legislation and therefore have to comply with the law.

Therefore, the U.S. cloud providers might not be able to re-establish trust in their company without any changes to the U.S. legislation and surveillance practices. Even if the U.S. government decided to stop all surveillance activities and change the law accordingly, it would probably take a long time until the German buyers decided to trust the U.S. cloud providers again. Lost trust, especially in this area, cannot be regained that quickly". Furthermore, according to Krishnan et al. (2006), trust reduces the likelihood of negative interpretations of the actions of the other party by allowing

for the benefit of the doubt. However, since the German companies did not have much trust in the U.S. cloud providers even before the global surveillance disclosures, the negative press about the involvement of U.S. cloud providers in the surveillance activities (Section 2.2.2) were probably not be interpreted in a positive way.

Company reputation

Independent of the relationship to a single individuum in der buyer's or seller's organisation, bilateral relational norms and corresponding informal monitoring mechanisms are important to build trust between both organisations and improving market performance (Aulakh et al., 1996). According to Kwon and Suh (2004), the reputation of a business partner has a strong positive impact on the level of trust. However, the authors argued that it takes time to build a reputation in the market. To build a positive reputation, suppliers need to gain the perception that they are honest, deliver quality products/services and keep their word (Maister, Green, & Galford, 2000). Since cloud computing is a relatively new product/service, potential buyers do not have much historical information that they can base their decisions on. It could therefore be beneficial for U.S. cloud providers to proactively inform potential customers with helpful information. This could include certain independent industry or government certificates, transparency initiatives such as data centre visits and audits performed by sovereign organisations that the buyer organisation can rely on.

Another aspect that the cloud sellers considered important was to have references, case studies and customer success stories from customer that were in the same sector and that shared similar challenges. Aulakh et al. (1996, p. 1026) maintained that this open information exchange can have "a positive effect on the trust between the firms as well as enhance partnership performance". Sako and Helper (1998) also provided empirical support that information exchange and technical assistance have a significant effect on facilitating the creation and sustenance of trust. However, as discussed in Section 6.1.2, the dynamics of these trust relationships are guided by the regional cultural practices and sales managers need to take the national cultural differences into account "in order to avoid pitfalls" (Aulakh et al., 1996, p. 1026). Section 6.3 will discuss additional thoughts how U.S. cloud providers can improve the buyer-seller trust relationship form the perspective of the German buyers.

As mentioned earlier, U.S. cloud providers already started with implementing some of the measures proposed by the key informants. This includes the provision of local cloud data centres in Germany and the implementation of strong encryption technologies. The fact that U.S. cloud providers are already implementing some of these suggestions supports the findings of the current research and is a strong indicator that the concerns of the German companies are substantial and have a significant monetary impact on the providers' businesses. It also shows that sellers need to carefully listen to and understand the fears and concerns of their potential customers and keep in mind that these can differ significantly depending on the country and cultural background of the buyer.

A key policy priority of U.S. cloud providers should therefore be to plan for the long-term care of their German customers by (re-)building trust step by step. Therefore, U.S. cloud providers need to solve any trust issues first before they can steer the conversations with their customers from an emotional level and gut decisions to an evidence and hard facts-based discussion. This could for example be reinforced by building strong reference cases in terms of successfully implemented public cloud projects for each target sector. As mentioned by some of the cloud seller respondents, German customers are closely observing what their peers in their industry are doing because none of them wants to be the first one taking the risk. The relatively slow public cloud services adoption in Germany could thus be accelerated by financially supporting public cloud migrations and proof-of-concept projects with carefully selected enterprise customers in Germany. Another approach could be to arrange visits for German customers to the data centre facilities of U.S. cloud providers. This would give German customers an opportunity to experience the security measures at first hand and ask questions about the storage and processing of their data.

6.2.2.2 German cloud providers

Both buyers and sellers expressed the sense that German cloud providers would try to take advantage of the global surveillance disclosures and position their cloud offerings as more secure than the services provided by U.S. companies. According to the sellers, the German cloud providers proactively advertised their cloud services as "made in Germany" and labelled their outsourcing offerings as cloud services. This confirms the observation described in Section 2.3.4 that German cloud providers

actively advertised the fact that data stored with a German cloud provider would be safe from access by the U.S. intelligence agencies. It could therefore be argued that the environmental uncertainty regarding the potential access of U.S. government agencies to data stored at U.S. cloud providers gave German cloud providers an exclusive selling proposition. El-Gazzar (2016) came to a similar conclusion and found that because of the Snowden leaks and the influence of the media, global cloud providers would represent a risk for many cloud consumers. The author argued that the local providers have demonstrated their adherence to government regulations and interpreted this behaviour as a mimetic pressure which was lacking in previous literature (S. Schneider & Sunyaev, 2016).

Environmental uncertainty

In order to build long-term oriented buyer-seller relationships, trust needs to be established (Ganesan, 1994). This is, however, not the case if the buyers cannot evaluate if they can trust the U.S. cloud providers or if this is impossible due to U.S. government interference. The study by Krishnan et al. (2006, p. 909) revealed that at high levels of environmental uncertainty “the trust-performance relationship disappears and possibly reverses”. Environmental uncertainty results from exogenous sources outside the scope of the buyer-seller relationship (Bergh & Lawless, 1998; Buchko, 1994; Dess & Beard, 1984) and can for example be caused by product-market instability (Aldrich, 2008; Dess & Beard, 1984; Wholey & Brittain, 1989). Speedy and responsive decisions are required to adjust the business strategy accordingly (Huber, Miller, & Glick, 1990; Mintzberg, 1978). The global surveillance activities could be seen as an environmental uncertainty which exists outside the control of the U.S. cloud provider and the German buyer company but have a strong impact on the trust between both parties. This would support the findings of Krishnan et al. (2006) that environmental uncertainty can have a strong negative effect on the trust relationship between business or alliance partners. It could therefore be argued that U.S. cloud providers should focus on taking measures to protect the buyer-seller relationship from these negative external influences and lower the degree of uncertainty for the buyers.

Practitioner surveys following the global surveillance disclosures found that the trust of cloud customers in U.S. cloud providers had decreased but buyers were undecided

about their future cloud strategy. A study of PwC (2013b, p. 23) showed that after the revelations of Edward Snowden, 15% of the surveyed companies considered changing their cloud provider to a “European IT service provider that is not under suspicion of cooperating with U.S. or British intelligent agencies”. However, most of the respondents (69%) were not planning to change their current cloud provider. Three out of four cloud providers surveyed in the study of PwC (2013a, p. 31) stated that “the relationship between customers and providers will change dramatically” and that this will “forge new demands on vendor management”. However, the study did not reveal what exactly will change and what the new demands are. In another study conducted by KPMG (2014), almost two-third of the companies surveyed by reported that their trust in cloud providers had decreased because of the NSA espionage incidents. The authors of the study concluded that cloud providers were therefore “facing the challenge” to “counteract the damage to their reputation” and to win back the trust of their customers with “trust-building measures” (KPMG, 2014, p. 32). In comparison, the trust in conventional IT service provider and telecommunications provider showed considerably less loss in trust because of the NSA incidents. As argued by Ganesan (1994, p. 14), “insufficient understanding of a customer’s orientation can lead to problems, such as attempting to form a long-term relationship”. It would therefore be vital for U.S. cloud providers to understand the factual and emotional reasons why German customers lost trust in U.S. cloud providers in order to build a long-term business relationship.

Emotional factors

A few buyers acknowledged that storing company data in a German data centre might be mainly based on the gut feeling of the decision makers of the German companies. It could hence be argued that the preference of German companies for German cloud providers was not primarily based on factual knowledge but rather on the personal gut feeling of the decision makers. Additionally, as maintained by the buyers, several of their own customers demanded that their data was not allowed to leave Germany and that their customers were afraid of getting involved in any kind of data privacy scandal. They explained that this requirement was not because of legal requirements but mainly driven by fear and that their companies could use this condition to differentiate themselves from the competition. As discussed in Section 6.1.2, the German culture

has a high score on the uncertainty avoidance scale by Hofstede (2018) which includes avoiding risks. For example, several buyers used the word “Angst” to describe the risk of economic espionage for their business when using U.S. public cloud services. It could therefore be possible that the German cloud providers made use of this cultural characteristic for their own purposes by instilling fear in U.S. cloud services and by publicly commenting that the NSA could not access their data centres. The findings suggested that the trust of German companies in German cloud providers was higher than in U.S. cloud providers or in public cloud providers from other European countries. However, in case of the buyer respondents of the current research, the marketing initiatives of the German cloud providers did not produce the desired effect. Instead, as it will be discussed in the following section, the German companies chose to keep their data on-site in their own data centres.

The speed of the development in cloud computing technologies is breath-taking. The largest public cloud service providers Amazon (2017a), Google (2017a) and Microsoft (2017a) are announcing new features and functionalities of their services on an almost daily basis. As one can see from the annual reports of these companies, the major players on the market are doubling their business revenue with cloud services year over year and are consequently duplicating their data centre capacities accordingly. U.S. cloud providers develop their own specialised hardware for cloud data centres (Vaid, 2016), develop reprogrammable computer chips for artificial intelligence applications (Metz, 2016) and become the largest owners of intercontinental submarine network cables (Sverdlik, 2017). The largest German and European information technology company, SAP, is considerably smaller than its American counterparts. The market capitalization of U.S. IT companies such as Apple, Google or Microsoft is about five time larger than the value of SAP (Chazan, 2017). Moreover, SAP is not only providing their own cloud services but also relies on the infrastructure of large U.S. cloud providers. For example, SAP customers can run their applications in data centres from Amazon (2017b), Google (2017b) and Microsoft (2017b). This shows that even Europe’s largest software and IT company is dependent on the services of U.S. cloud providers.

However, as outlined in the background chapter, the cloud computing technology and business model is still in its infancy and will most likely be subject to several

innovations and changes over the upcoming years. A current technological development which is strongly interconnected with cloud computing is artificial intelligence. Cloud providers started to offer artificial intelligence and machine learning algorithms as a service to enterprises and start-up companies and give them the opportunity to innovate on the shoulders of the internet giants (Waters, 2016). Artificial intelligence, however, also bears unforeseeable risks (Gibbs, 2014). Already today, humans have difficulties to comprehend the interconnected layers of artificial deep neural networks (Knight, 2017). For example, Jack Ma, the founder of China's largest internet company, believes that artificial intelligence "will cause people more pain than happiness" (Solon, 2017). Therefore, influential individuals such as Elon Musk and companies such as Amazon and Microsoft are sponsoring OpenAI (2015), a non-profit research company working on safe artificial intelligence models. As with public cloud computing, "the U.S. appears to be leading the revolution" in artificial intelligence (O'Keefe & Rapp, 2017) and European or German companies are rarely cited in the reports about artificial intelligence businesses. This development will probably widen the gap between the capabilities of U.S. cloud providers and European or German cloud providers even more and will further increase the dependency of European and German companies on U.S. cloud provider companies.

6.2.2.3 Private cloud

Despite the business benefits of public cloud services presented in Section 2.1.3, the buyer respondents of the current research preferred to keep their data on-site in their own data centre. A survey conducted by KPMG (2014) revealed that only 15% of the companies in Germany were using public cloud services while 36% invested in private one-premise cloud solutions. A more recent survey by KPMG (2017a) revealed that 29% of the respondents were using some public cloud services and 44% of the German companies said that they were building their own private cloud. Unfortunately, none of these surveys reported the percentage of the server systems that the companies moved to a public or private cloud platform and if they moved any of their core business applications to the public cloud. Therefore, even companies that only used a public cloud service for an uncritical service in terms of data privacy such as a public website became part of the statistic of companies that were using public cloud services. Additionally, the term private cloud is often misleading, and companies are

labelling their virtualized server infrastructure as their private cloud platform. However, this setup does not meet the definition of a cloud service as defined in Section 2.1.2. Nevertheless, after the global surveillance disclosures, even some researchers recommended to keep sensitive company data on premises. For example, Henze, Hiller, Hohlfeld, and Wehrle (2016) proposed decentralized private clouds to allow users to protect their privacy.

Decision-making uncertainty

As defined by Hofstede (2018) and discussed in Section 6.1.2.2, the German culture as a high uncertainty avoidance score. T. Gao et al. (2005, p. 397) argued that "organizational buyer's decision-making uncertainty" has a negative effect on purchase behaviours and needs to be reduced. The researchers found that when the buyers perceive their suppliers as trustworthy, they report lower decision-making uncertainty. This is consistent with prior research (e.g. Morgan and Hunt (1994) and J. B. Smith and Barclay (1997)) suggesting that trusting involves vulnerability on the part of the trustor and that a trusting party tends to make risky decisions. T. Gao et al. (2005, p. 401) summarised that "trust leads exchange partners to make 'risky' decisions because they perceive the situation as having less uncertainty". It could therefore be argued that German companies would potentially make more risky decisions, for example by moving their data to a public cloud provider, if they trust the selling organisation. However, since the German buyers commented that they would not accept any risks, they would probably not decide to move their corporate data to a U.S. cloud provider.

Furthermore, the key respondents of the German companies explained that they preferred having the IT systems and staff under their direct control because their own IT departments would understand and support their business model very well. As discussed in Section 4.4.5.1, staff working at the companies' internal IT departments could be worried about losing their jobs when IT services get outsourced to external cloud data centres. The argumentation that companies could lose technical skills could therefore be driven by IT staff members to keep their jobs.

However, in contrast to the buyers, the sellers argued that the IT departments of the German companies and especially SMEs were not able to provide IT services with the same level of quality and security as the services provided by the U.S. cloud providers.

The sellers claimed that their customers would understand that they could not compete with cloud security and that that most data leaks would come from inside an organisation. This confirms the assessment in Section 2.1.5, that SMEs often do not have the needed resources and know-how or cannot achieve the necessary economies of scale to achieve a sufficient level of security. Likewise, El-Gazzar (2016) found that cloud service providers would argue that the security of cloud services was much higher than the security of local data centres. For example, a cloud provider argued that it was irrational to think that data security was more secure in the local data centre than “having data stored with the best security providers in the world”. Likewise, a respondent from another provider maintained that “the local IT departments do not have skills with regard to security to be able to protect the company” (El-Gazzar, 2016, p. 146).

Investment costs

As argued by Dyer and Chu (2000), buyers incur substantial costs in developing high trust supplier relations. In the long term, buyers may get a return on their investments in the form of more effective business processes and higher profits. However, in case of public cloud services, they still must incur the expense of software and data migration and a change of the necessary skills of their internal staff. Additionally, in case the buyer needs to change the supplier, “the effort required to find, evaluate, and select a new supplier” might be “too time-consuming and expensive” (Handfield & Bechtel, 2002, p. 376). Therefore, since “building supplier trust imposes costs on buyers” (Dyer & Chu, 2000, p. 279), German companies might choose to leave their data and compute services on premise and only consider public cloud services if the business benefits of the public cloud as outlined in Section 2.1.3 do not outweigh the perceived risks and the upfront and continuous investment costs.

Additionally, several buyers of the German companies argued that they did not believe that they would save costs when moving to a public cloud service. This contradicts, however, the statements of some of the buyers in Section 5.4 and the practitioner literature cited in Section 2.1.3 that one of the key motives for adopting cloud technologies was cost savings. The sellers, on the other hand, claimed that German companies were too proud of their own IT competencies and would think that they could provide services that were as good or better than U.S. cloud services. This

reflects the discussion in Section 6.1.2 about the cultural characteristics of German companies in terms of taking a pride in their own engineering capabilities and distrust in the quality and security of the services offered by U.S. cloud providers. As argued by Mauerer (2016), in Germany, the "country of engineers", technical solutions need to be fully developed and matured. Therefore, apart from the concerns resulting from the global surveillance disclosures, German companies might have a general tendency to keep their data and knowledge in-house instead of finding a contractual agreement with an outsourcing partner. However, as found by Hoffmann et al. (2010, p. 112), companies that have managed to develop a trustful relationship with other companies "have a fundamental strategic advantage" and gives the companies the option to focus on their core business and "organize certain activities more efficiently and flexibly with exchange partners".

Digital transformation

At about the same speed as cloud technologies develop, traditional business models are disrupted by small start-up companies without tangible assets and with small capital investments. As summarised by a technology journalist in 2015,

> *"Uber, the world's largest taxi company, owns no vehicles. Facebook, the world's most popular media owner, creates no content. Alibaba, the most valuable retailer, has no inventory. And Airbnb, the world's largest accommodation provider, owns no real estate." (Goodwin, 2015)*

These businesses can be run almost completely in the public cloud and automatically scale up and down according to customer demand. Companies in Germany are trying to prepare themselves for the "digital revolution" (Gaycken, 2017) by large investments in the "digital transformation" (SZ, 2017) of their businesses. In addition, the term "Industry 4.0" describes a trend in the manufacturing industry to include cyber-physical systems, the internet of things and cloud computing in the industrial process. Since the German economy depends on exports of high technology goods and the manufacturing industry is one of the most important sectors in Germany, the Federal Ministry of Education and Research is supporting this initiative in order to maintain the competitiveness of German industry (BMBF, 2015).

The “digital revolution” affects almost any business and new innovative business models can render traditional enterprises or even entire sectors obsolete. Most of the large companies in Germany are from traditional industries such as manufacturing, retail and chemicals (Chazan, 2017). The challenge for the German economy will be to transform these businesses in a way that makes them relevant and profitable for the next decades. Prominent examples for this competition are Silicon Valley companies developing autonomous vehicles that will eventually compete with the German car manufacturers (Ewing & Scott, 2017). The development of autonomous cars and the Industry 4.0 may become a problem for Germany if German companies are only delivering the engineering components and Silicon Valley companies provide the brain in terms of software and artificial intelligence systems.

A reasonable approach for German companies to tackle this issue could therefore be to constantly challenge their attitude towards public cloud services and assess the risks versus the benefits for their businesses.

6.2.2.4 Summary

All three findings regarding the second trust relationship, company trust (RO2b), suggested that German companies did not trust U.S. cloud provider companies with their data. These findings have several implications. Firstly, it became clear that the NSA surveillance activities had a strong negative impact on the trust of German companies in U.S. cloud provider companies and that U.S. cloud providers had to actively work on measures to win back the trust of German businesses. As discussed above, ethical behaviour of the selling company and the salesperson may have a strong impact on the trust in the salesperson and the reputation of the selling company.

Secondly, since most of the German companies preferred to keep their data on-site, it could be argued that the marketing campaign by the German cloud providers did not convince their German customers to use their cloud data centres. As debated above, this could be due to the overall environmental uncertainty and the emotional reactions caused by the global surveillance disclosures. Therefore, the German cloud providers are less of a competition to the U.S. cloud providers than the private cloud initiatives of their potential German customers.

And thirdly, in accordance with previous studies, German companies preferred to store their data in their local data centre. A probable reason for this behaviour is the investment decision uncertainty triggered by the surveillance scandal and the fear of getting locked-in to an inflexible cloud contract. Consequently, to convince their German customers to not invest in private cloud infrastructure but to move their IT to public cloud services, U.S. cloud providers need to educate the German market about the advantages of public cloud solutions and build trust in the security of their public cloud offerings.

6.2.3 Salesperson trust (RO2c)

Two divergent and often conflicting discourses emerged from the question if the German cloud buyers trust the local sales representatives of the U.S. cloud providers. The first section will address the importance of the local sales representative of the U.S. cloud providers for the purchase decision of the German companies regarding U.S. cloud services. The subsequent section will elaborate the opinion of the cloud buyers and sellers regarding the significance of German market and sector knowledge and experience for public cloud services adoption and discuss these contradictory assertions.

6.2.3.1 Local sales representatives

One of the key findings regarding salesperson trust was that most of the buyers of the Germany companies stated that they did not see much value in the work of the local sales representatives of the U.S. cloud providers. These findings, however, did not support previous studies. As detailed in Section 3.4.2, previous research found that the role of the salesperson and the trust in the salesperson were important to the buyers (e.g. Dwyer et al. (1987)). Some studies even identified salesperson trust as the most important variable of all trust relationships (e.g. Ganesan and Hess (1997)). For example, Swan et al. (1985, p. 203) found that “trust increases as the customer gains the impression that the salesperson is dependable, honest, competent customer oriented and likeable”. Furthermore, Crosby et al. (1990, p. 68) maintained that, more often than not, “the salesperson is the company” and that the “salesperson is the primary – if not the sole – contact point for the customer both before and after the purchase”. Trust was also found to be a critical attribute when the buyer must decide between competing salespeople (Swan et al., 1988). As argued by Jon M. Hawes et

al. (1989, p. 1), the career of a salesperson is very much dependent on his or her ability to “earn, enhance, and retain the trust of potential and current customers”. Moreover, from a list of 25 salesperson characteristics, Jon M. Hawes et al. (1993) found trustworthiness to be of greatest importance.

Impact of salesperson trust on company trust

The answers of the buyers of the Germany companies suggest that the local sales representative of the U.S. cloud providers did not add much value and could not improve the view of the buyer in the selling company. From their point of view, U.S. companies were highly centralised and controlled from the corporate headquarters and the salespeople did not have any decision power. However, the findings of the current study do not support the previous research. Several studies found that the salesperson was not only a representative of the selling company but would also have a significant impact on the trust relationship between the buyer and the selling company. In contrast to A. Zaheer et al. (1998) who argued that inter-organizational trust was the dominant influence on performance, M. Srinivasan and Srivastava (2012) concluded that trust of the buyer in the salesperson would lead to trust between the buyer and the selling organisation. Similarly, Ashnai et al. (2016) concluded that building trust with individuals in the buying company would lead to overall trust between the organisations. The authors recommended that relationship managers should focus not only on building inter-organisational (company) trust, but also on building personal trust with individuals of the other organisation. According to Ashnai et al. (2016), salesperson trust will also lead to increased information sharing between the companies and in turn to increased commitment and performance. Especially in situations when the buyer has no prior knowledge of the brand or when the buyer has low expectations of the brand, the credibility of a salesperson could have a positive effect on product evaluation and buying intention (A. Sharma, 1990).

The sellers, on the other hand, claimed that German companies demanded a local contact who could speak German and that their customers preferred to talk to someone in Germany and in the local language. Hence, the opinions of the buyer and seller on the positive influence of the salesperson on the trust of the buyer in the selling organisation or the product/service were contrary, and it may depend on the specific customer situation if the salesperson is seen as a valuable resource to the buyer.

Personal relationship

The buyer respondents stated that the personality of the salesperson would not have much influence on their purchase decision. Additionally, they argued that the local sales representatives of U.S. cloud providers in Germany had not enough power to make important decisions and had no substantial impact on the design and configuration of the cloud products. The sellers, on the other hand, argued that a personal relationship between sellers and buyers was of the utmost importance and that technology would be secondary. This is another example of conflicting views of the buyer and seller respondents regarding the importance of building a personal relationship with the salesperson.

Previous studies also found that building a personal relationship between salesperson and the buyer would be critical for building trust relationships between the parties. For example, Newell et al. (2011, p. 314) argued that sales relationships have a “very strong interpersonal dimension in which an emotional bond between parties can be established”. Therefore, by cultivating this interpersonal relationship, the buyer and the seller would develop stronger levels of trust and loyalty (Newell et al., 2011). D.-J. Yang and Wu (2014) went even further by claiming that the social competence of a salesperson could have a stronger effect on salesperson performance than professional competence. In a more recent study, M. Srinivasan and Srivastava (2012, p. 31) confirmed the findings of e.g. Kumar et al. (1995), Jule B Gassenheimer, Houston, and Davis (1998) and R. L. Oliver and Swan (1989) of “a positive relationship between salesperson benevolence and buyer’s perceived equity with the salesperson and trust in the salesperson”. As argued by Chow and Holden (1997, p. 293), “customers will only purchase from companies when quality, price and service measure up”. However, “at an emotional level”, trust emerged as a critical factor in true customer royalty, product perception, openness of communication and purchasing behaviour (Chow & Holden, 1997, p. 293). T. Gao et al. (2005, p. 402) argued that the seller should “devote more time and resources” and “demonstrate the spirit of dedication and commitment” to the buyer” as these actions would most likely enhance buyer trust and reduce decision-making uncertainty. Such a commitment would provide evidence to the buyer that the seller can be trusted and is willing to make sacrifices to build and maintain the business relationship (Doney & Cannon, 1997).

Furthermore, several studies identified communication and information as helpful in building trust between the buyer and the salesperson. Coote et al. (2003, p. 601) found that “the effect of communication on commitment was strongly positive” and that “there was consistent support for the communication → trust relationship”. The authors recommended that managers (or sales representatives) seeking to build commitment and trust should encourage the exchange of accurate and meaningful information and avoid the exchange of harsh words. Moorman et al. (1993) also identified communication as a key factor to improve trust. Similarly, Kwon and Suh (2004, p. 4) found that “information sharing reduces the level of behavioural uncertainty, which, in turn, improves the level of trust”. Additionally, several authors argued that, as the buyer’s trust in the salesperson grows, so too does their willingness to share information and purchase the products or services of the selling company (e.g. J. C. Anderson and Narus (1990), Celuch et al. (2011), Wood et al. (2008), Vidal and Goldenberg (2014), Ashnai et al. (2016)). This finding supports the proposition that local sales representatives are important to engage in communication with German buyers in the local language to build trust in the organisation and products of the seller’s company. Several seller respondents commented that sharing customer references and information about how other companies developed their cloud strategy were received positively by their customers. However, as argued by Kwon and Suh (2004), “simple information sharing may not be enough to overcome barriers and suspicion” and suppliers should build a reputation based on quality products/services and a positive track record with other relevant customers.

Self-service

Several buyer respondents stated that they would inform themselves about a product or service without the need of a salesperson. The buyers argued that they were primarily interested in the product itself and that the salesperson would not change their opinion about it. Kennedy et al. (2001, p. 82) found that buyers “who perceived themselves as knowledgeable about the product prior to its purchase had lower levels of trust of the salesperson”. The authors recommended that sellers should be prepared for meeting highly knowledgeable customers through training and preparation. The features and configuration details of public cloud services are generally well documented and potential buyers can theoretically inform themselves about the

services of a public cloud provider in detail before meeting with a sales representative. Kennedy et al. (2001) suggested that buyers who have taken the time to understand a product or service themselves may have less need for a salesperson and that with the widespread information availability on the Internet, the product knowledge of potential buyers will likely increase.

Additionally, public cloud provider such as Amazon Web Services and Microsoft Azure allow customers to purchase cloud services directly from an Internet web portal by entering their credit card number and personal information. As reported by some of the sellers, small businesses would buy cloud serviced directly online. Moreover, small start-ups and companies in the media industry prefer to do large parts of their business online and therefore have no need for a personal relationship with a local sales representative. According to 19% of the cloud providers interviewed in the study of PwC (2013a, p. 31), the relationship between the local salesperson and the cloud provider will become less important because “in the future, more and more cloud providers will opt for an internet sales model” and therefore will “not employ their own sales personnel” anymore. In the opinion of the authors of the study of PwC (2013a, p. 33), it is likely that cloud providers will employ a “hybrid form of distribution” by offering their products and services on the internet as well as through their own salespeople. Therefore, buyers can already purchase cloud services without the interaction with a salesperson and this distribution channel could become even more popular in the future.

In addition, buyers might view any help from a salesperson as more of an “attempt to persuade or unduly influence” them in their decision-making process (Kennedy et al., 2001, p. 82). Hence, sales representatives are advised to understand how to appropriately approach buyers that seek information themselves before making purchases (Kennedy et al., 2001). However, the sellers maintained that enterprise customers would prefer a local sales representative to talk to and that they would not buy U.S. cloud services without this personal relationship. This is in line with the discussion above, that the size of a company has an impact on the needs of the buyers.

Selling orientation

Furthermore, the buyers expressed their concerns that the sellers would make promises they could not keep and possibly try to downplay the risks of using U.S. cloud services. This could potentially be another reason why the German buyers were not interested in the help of a salesperson. If their view is that the sole intention of the salesperson is to convince them to buy their products and if they do not see any value in the consultancy work and explanation of the products and services, the buyers might want to read about the product features themselves and buy through different channels such as the provider's website or a local partner.

The literature on salesperson trust also suggests that salespeople should be cautious with putting too much pressure on buyers or with making false statements. Selling orientation is typically seen as a form of "hard selling" (Guenzi et al., 2016, p. 555) including manipulative tactics aimed at maximizing the interest of the seller, even at the expenses of the buyer (Delvecchio, Zemanek, McIntyre, & Claxton, 2004). Therefore, when selling orientation is high, buyers might assume that the salesperson is using manipulative strategies to close the immediate sell, which will probably lead to low trust in the salesperson (DeCarlo, 2005). Kennedy et al. (2001) also suggested that salespeople should use low-pressure selling tactics and take service quality and ethical concerns into account to improve buyer-seller trust. Likewise, Guenzi and Georges (2010, p. 114) found that "selling orientation has a negative impact" on buyer trust in the salesperson and Tam and Wong (2001) demonstrated that selling orientation has a negative effect on customer trust and customer satisfaction while customer orientation influences them in a positive way. Additionally, a study conducted by Strutton et al. (1996) found that self-enhancement and self-promotion were negatively associated with the level of trust buyers placed in the salesperson. The authors recommended that sales managers should discourage the use of favour-rendering, especially in the early stages of a relationship.

According to Friend et al. (2018, p. 5), the "higher a customer's propensity to trust, the greater his/her trust in the salesperson". Hence, according to the authors, buyers with a low propensity to trust are less likely to trust the salesperson. Therefore, in a situation when the customer has less reason to trust the salesperson or his/her company, it might be particularly difficult for the sales representative to build a trust relationship

with the buyer. The global surveillance disclosures probably did not enhance the German buyer's propensity to trust in U.S. companies or, still less, in U.S. cloud services. Following this reasoning, the local sales representatives of the U.S. cloud providers should perhaps keep in mind that the German buyers might be in general less motivated to trust them, their employer and their products and give the German sellers time to process the surveillance incidents.

However, not all studies found that salesperson trust had a positive influence on purchase behaviour in all situations. For example, Doney and Cannon (1997, p. 45) found that "current supplier selection is not influenced by trust of the supplier firm or its salesperson". A possible explanation could be that professional buyers are trained to focus on objective facts rather than on subjective assessments of trust (Doney & Cannon, 1997). Nevertheless, the authors maintained that trust of the salesperson and the selling company do increase the likelihood that buyers anticipate doing business with the seller in the future. In conclusion, Doney and Cannon (1997) recommended selling organisations to make investments to develop and maintain buyer trust and that the outcomes would be critically important to supplier firms.

As summarised by Oakes (1990), salespeople are in a permanent conflict. On the one hand they need to build a trust relationship with their customers to be able to sell goods and services to them and, on the other hand, the constant sales pressure and the constraint to maximize sales profits jeopardizes this relationship (Oakes, 1990). The following section will discuss the importance of salesperson expertise in terms of market and sector knowledge for the German IT purchase decision makers.

6.2.3.2 Market and sector knowledge

Another key finding regarding the trust in the salesperson was that the buyers of the German companies stated that the local sales representatives of the U.S. cloud providers should have great knowledge about cloud computing technologies, national particularities as well as familiarity with the sector or industry their customer was in. This is, however, in contrast to the findings in the previous section where the respondents of the German companies stated that they did not need a local sales representative of the U.S. provider and that they did not trust their statements. On the one hand, the interviewees of the German companies claimed that they did not trust the local sales representatives of the U.S. cloud providers and, on the other hand, they

argued that U.S. cloud companies should employ people in Germany who know the specific characteristics of the German market and the sector of the customer they want to do business with.

Expertise

The cloud sellers agreed with the respondents of the German companies that product and industry knowledge would be essential for doing business with German enterprise customers. The connection between expertise and trust between buyers and sellers has been investigated in a number of studies. To a large extent, sales literature has viewed salesperson expertise positively, suggesting that higher levels of product and industry knowledge are beneficial to the trust in the sales representative. The expertise of a salesperson could be defined as the “knowledge, technical competence and ability to provide answers to specific questions” (Guenzi & Georges, 2010, p. 119). Research indicates that the expertise of a sales representative may help developing trust by creating confidence in the buyer that the salesperson is knowledgeable (e.g. Moorman et al. (1993), A. H. Liu and Leach (2001), Dowell, Heffernan, and Morrison (2013)). As argued by Crosby et al. (1990) and Swan et al. (1999), the expertise of a salesperson could reduce the buyer’s feelings of uncertainty and vulnerability and should therefore be a predictor for the buyer’s trust in the salesperson.

This study produced results which corroborate the findings of a great deal of the previous work in this field. As one of the first studies on this subject, Busch and Wilson (1976, p. 10) found that “the stronger the expert and referent power bases the more trustworthy the salesman was perceived to be by the customer”. Moreover, the expert power was even more important than the referent power as a factor improving trust. Likewise, Doney and Cannon (1997, p. 47) maintained that “buyers trust salespeople they perceive to be expert” and that buyers might think that “expert salespeople can deliver on their promises”. Similarly, A. Sharma (1990) recommended that sales representatives should provide their customers with information that can be supported by independent unbiased experts to increase their perceived trustworthiness. According to Kennedy et al. (2001, p. 81), a “competent salesperson with complete and accurate product knowledge” creates satisfaction and trust of the salesperson and the selling company because buyers would intuitively associate a salesperson with his or her parent company.

Wood et al. (2008, p. 279) performed an analysis of 32 studies that measure trust-related constructs in the context of a buyer's assessment of a seller and revealed that "one seller characteristic – expertise – positively influences a buyer's trust". Furthermore, the authors found that the buyer is looking for a specific attribute to categorize if a seller is either a member or a non-member of his or her trustworthy group and that this evaluation would have the greatest impact on trust. However, since Wood et al. (2008) based their research on secondary data it might not be guaranteed that all studies that were analysed shared the same understanding of the naming and scales of measures to make the studies comparable. A more recent study conducted by Guenzi and Georges (2010, p. 114) show that "both salesperson's customer orientation and expertise positively influence customer trust in the salesperson". This also seems to be the case with other cultures such as China, where Newell et al. (2016, p. 160) found that "trust and expertise play key roles in developing long-term business-to-business associations". However, as argued by Hofstede (2003a), China has a much higher collectivism score than German or the U.S. which should be taken into account when comparing the countries. Shepherd, Gardial, Johnson, and Rentz (2006, p. 132) found that expert salespeople would reach better decisions faster and recommended "on-the-job training programmes" as well as classroom trainings. In case of U.S. public cloud services, U.S. cloud providers may be able to improve the trust of their customers by hiring skilled experts and providing additional training to their current staff.

However, not all studies came to the conclusion that expertise was an important factor for salesperson trust. Jon M. Hawes et al. (1989, p. 6) found that "being likeable, competent, or dependable" were not as important in trust development for buyers as the sales managers expected. For example, purchasing managers rated competence (e.g. product knowledge) as significantly less important than sales managers. This was also the case with other attributes such as personality and likeability. Other authors argued that expertise would only have the desired effect on salesperson trust if it was used in combination with a strong emotional connection. For example, Newell et al. (2011) argued that while expertise and competency are important factors for buyer-seller trust, their study showed that without a strong emotional (interpersonal relationship) connection, trust and loyalty to the salesperson and the selling company would be significantly reduced. Consequently, salespeople should focus on "analysing

the buyer's business-related needs and to develop creative solutions" (Newell et al., 2011, p. 313).

Importance of purchase decision

As reported in Section 2.1, the decision for cloud computing services can have an impact on the IT strategy and the corporate strategy of the buying company and could therefore be rated as an important purchase decision. From the point of view of the sellers, there was no doubt that cloud services would be the future for any business and that it was only a matter of time. Belonax et al. (2007, p. 252) found that "buyer perceptions of supplier and salesperson expertise and trust were higher when the purchase was minimally important than when the purchase was extremely important". Purchase importance can be defined as "the buying firm's perceptions of the strategic significance of a particular purchase to the organizations objectives" Hutt and Speh (2001, p. 93). Belonax et al. (2007) suggested that this phenomenon could be explained in two ways: First, buyers might be less willing to make a quick decision in situations when the purchase is more important and that the attributes of the product or service play a more prominent role in the buyer's decision than the expertise and trust of the salesperson. Second, because of the repetitive and routine nature of low-importance decisions, the buyer is more likely to act on criteria that enable effortless decision making and the trust in a salesperson might represent criteria that allows quick low-importance decisions (Belonax et al., 2007).

The implication of this finding regarding public cloud services could be that in cases where the buyer sees purchasing public cloud services as a decision of high importance, public cloud providers would need to convince the customer with product features and quality. Hereafter, once the customer is satisfied with the overall product line of the cloud service provider, salespeople could build a long-term relationship with the buyer and might have a better basis for recommending and selling additional products and services. However, a possible limitation of this study was that the respondents could decide for themselves which purchase decisions they rate as important or unimportant. Guenzi et al. (2016) maintained that salespeople willing to win buyer's trust should modify their sales approach across the relationship lifecycle. They argued that when purchase importance is low, salespeople should combine an adaptive selling approach with a low selling orientation tactic. However, when

purchase importance is high, the interaction between adaptive selling and selling orientation becomes less significant although selling orientation is still negatively related to trust (Guenzi et al., 2016).

In addition to the importance of the purchase decision, the supply risk could also have an impact on the trust in the salesperson. M. Srinivasan and Srivastava (2012) claimed that “higher supply risk resulted in a stronger positive relationship between salesperson benevolence and trust in the salesperson”. They argued that their results confirmed the findings of Doney and Cannon (1997) that a buyer facing risk in a purchase situation would turn to its salesperson who the buyer believes is interested in helping the buyer. This would mean that if German companies would rate purchasing public cloud services from U.S. cloud providers as supply risk, German buyers would see a local sales representative as helpful and valuable. However, as discussed above, this contrasts with what the buyer respondents of the current research stated.

Therefore, further research on this decision-making factor and an application to public cloud services would be of interest to determine the role of salesperson-trust in this setting.

Training

The buyers also commented on the responsibility of U.S. cloud providers to hire and train their employees appropriately. This was shared by several authors who recommended that salesperson trust could be positively influenced by personnel training. According to marketing literature, learning orientation and training positively influence sales performance (e.g. Sujan, Weitz, and Kumar (1994), Shoemaker and Johlke (2002), J.-E. Park and Holloway (2003)). A number of studies recommended that companies should design training concepts to help their sales people building trust with their customers and become more competent and professional (Bateman & Valentine, 2015; Kennedy et al., 2001; Newell et al., 2011; Newell et al., 2016). As argued by Kwon and Suh (2004), relationship management skill is a critical element for increasing the likelihood that buyer-seller relationships are successful. The researchers recommended intensive training and education of existing decision makers to build this critical skill. Likewise, Swan et al. (1985) suggested that sales managers should invest in training their sales personnel in formal lectures or role

playing exercises to become more dependable, honest, competent, customer oriented and likeable in order to improve trustworthiness. Swan et al. (1988) concluded that salespeople who improve their skills in these areas will be deemed trustworthy by buyers and rewarded for their efforts. Similarly, A. Sharma (1990) and Jon M. Hawes et al. (1993) recommended that sales managers should increase the trustworthiness and credibility of the salespeople through education and experience.

Training, however, is not limited to product and industry knowledge and ethical behaviour alone; training also extends to adaptive selling techniques as salespeople need to learn how to establish the right level of relationship and interact effectively with the buyer in various situations (Delvecchio et al., 2004; Guenzi et al., 2016). As suggested by Cron, Marshall, Singh, Spiro, and Sujan (2005), training salespeople should focus on growth-related KSA training (knowledge, skills, ability) rather than on task-related KSA training. Additional training was recommended regarding the personal relationship and selling orientation issues discussed above. Salespeople should consequently be "taught the difference between offensive and defensive integration tactics" and the reasons why self-enhancement and self-promotion prove harmful to a trusting buyer-seller relationship (Strutton et al., 1996, p. 159). Moreover, the relevance of interpersonal (salesperson) trust suggests the need for more training in this area (Guenzi & Georges, 2010; Twing-Kwong et al., 2013) and training salespeople by developing their product knowledge and social skills could facilitate buyer trust (D.-J. Yang & Wu, 2014). Consequently, sales managers should place greater emphasis on training their staff to assess buyer perception of dependence (Jule B. Gassenheimer & Manolis, 2001), become more competent at using low-pressure selling (Kennedy et al., 2001) and develop better interpersonal communication skills to cultivate deeper and more personal connections with the buyer (Newell et al., 2011). Additionally, managers could give their salespeople more freedom to learn from their co-workers and share their knowledge across the entire organization (Menguc, Auh, & Kim, 2011).

The current research therefore contributes to the body of literature on adaptive selling (e.g. Weitz, Sujan, and Sujan (1986), Boorom, Goolsby, and Ramsey (1998), Franke and Park (2006), Román and Iacobucci (2010)) by confirming that customers require

salespeople to have relevant industry and product knowledge and understand the business of their customer.

Hiring

In addition to training investments, sales managers should try to recruit prospective salespeople who offer greater potential on these skills (Jon M. Hawes et al., 1993) and "screen for the social abilities that facilitate establishing and maintaining long-term interpersonal relationships", for example in role-playing situations (Crosby et al., 1990, p. 77). One area where training might take too much time is language skills. This was, however, a skill which was seen as essential by the sales representatives of the U.S. cloud providers. As stated by the sellers, it was critically important that they could speak German to their customers.

Another skill that was frequently mentioned was ethical behaviour. For example, Bateman and Valentine (2015) found that "increased customer judgments about the ethics of the salesperson based upon observed behaviour consistently lead to greater trust in the salespeople, and that ethical treatment also encourages stronger purchase intentions". They proposed that human resource departments can measure the ethics of job candidates by using special tests to determine levels of individual ethical development. Similarly, Guenzi and Georges (2010) recommended that sales managers should carefully select candidates for sales positions that provide the necessary skills and attitudes for building trustful customer relationships. Moreover, Lagace et al. (1991) extended the model of Crosby et al. (1990) and recommended that corporations should create an environment where the potential of unethical behaviour is at a minimum and that supervisors should act as a role model for ethical behaviour within organisations. As discussed in Section 6.2.2, ethical behaviour was suggested to have a noticeable positive impact on the trust of the buyer.

Furthermore, even if salespeople can be trained to engage with buyers on a personal level, it also depends on the natural ability to relate to others for building up long-term personal relationships. Hence, selecting the right talents also plays an important role in improving buyer's trust in the salesperson and the selling company. In addition to ethical behaviour, empathy was also found to have a positive effect on customer trust and satisfaction. Jaramillo and Valenzuela (2016) demonstrated that salesperson's empathy plays a critical role in influencing the view about their relationship with a

selling company and would eventually lead to supplier loyalty. The authors highlighted the importance of hiring empathetic salespeople that are genuinely interested in serving the customer. However, the authors also encourage sales managers to walk the talk and act as a role model for the desired skills. As recommended by Fang et al. (2008), managers can support trust-building efforts by providing coherent structure and strategy.

Long-term commitment

According to previous studies, sales managers should also give salespeople enough time to build a personal relationship with the buyer. J. B. Smith and Barclay (1997, p. 17) recommended that managers should leave their sales representatives “in territories longer to enhance relationship continuity” and increase “the perception of each other’s trustworthiness”. Additionally, literature also indicates that buyer's trust in a salesperson is an increasingly important factor, as organizations focus on building and maintaining long-term, strategic relationships with their customers (e.g. Ramsey and Sohi (1997), Nicholson et al. (2001), Ryu et al. (2007), E. Jones, Busch, and Dacin (2003), Guenzi et al. (2016)). As argued by A. Sharma (1990), positive past experience with the salesperson, the product/ service or the selling company can be a major determinant of salesperson credibility and trust. Moreover, as maintained by Dyer and Chu (2000, p. 279), a “high degree of stability of organizational personnel at both organizations may be necessary to produce relationship-based trust (embedded ties)”. Following their recommendation, sales organisations should establish long-term relationships with their customers by assigning salespeople that will build a personal relationship over a longer period and not focus on short-term business goals.

Moreover, according to the buyer respondents, sales representatives should get the decision-making power to negotiate with buyers directly instead of being dependent on anyone in the U.S. corporate headquarters. As stated by the buyers, the German companies had made negative experiences with the empowerment level of the local sales representatives. In case of U.S. cloud services, the seller organization should therefore consider hiring and assigning sales representatives in Germany to build up personal relationships over time to earn the trust of German enterprise customers and give the local salesforce enough decision-making powers.

However, the downside of a strong buyer to salesperson relationship could be that a salesperson leaves to work for a competitor or set up in competition on his/her own (A. Wong & Sohal, 2002). On the other hand, if sales managers change salespeople too often, “trust is undermined each time a salesperson is replaced” (A. Wong & Sohal, 2002, p. 45). Therefore, depending on the value of the salesperson to the buyer, sales managers of the cloud providers might need to find the right balance between giving salespeople the time to build long-term relationships with their clients and at the same time make sure that they are not losing the customer in case that the salesperson is leaving to work for a competitor. In order to secure the trust-relationship with the selling company, cloud providers could try to deliver excellent product quality and aftersales service to stand out from the competition.

The current research includes a contradiction or paradox that could not be entirely explained or resolved. On the one hand, the key respondents of the German companies claimed that they did not need the help of local salespeople from the U.S. cloud providers. However, on the other hand, they argued that knowledge of the German market and industry know-how would be a requirement for doing business with them. This study could only speculate about the reasons why this was the case and it will require additional research to answer the question how much sales support will be necessary and accepted by the German decision makers and if German companies will purchase cloud services directly from the cloud providers’ websites in the future.

6.2.3.3 Summary

According to the buyers, a local sales representative does not positively influence their purchase decision. This is, however, in contrast to previous research which found that the salesperson has significant impact on the trust relationship between the buyer and the selling company. Previous studies also found that building a personal relationship between salesperson and the buyer would be critical for building trust relationships between the parties. One reason for this disagreement could be that the nature of public cloud services allows potential buyers to purchase cloud services online without any salesperson interaction and once a potential buyer feels informed and secure enough to make the purchase, they can buy the cloud services directly from the provider.

Nevertheless, the buyers argued that it was important that the salesperson was knowledgeable about their business and sector. This is in accordance with previous research which found that the expertise of a salesperson may help developing trust in the sales representative and the selling company. Moreover, as discussed above, salespeople should avoid hard selling methods and instead build long-term personal relationships with buyers to create trust. These skills can either be improved by training initiatives or through hiring salespeople with the required abilities.

Previous research has not involved cloud computing services as the product/service that is offered by salespeople. Future research should focus on the role of the salesperson in situations where buyers can both inform themselves online and buy the product/service online and find out what skills and selling methods have the highest impact on the trust and purchase intention of the buyer.

6.2.4 Foreign government trust (RO2d)

The following four sections will discuss the key themes that contribute to the understanding of the trust of the buyer in the foreign government (RO2d). The first section will assess the impact of the global surveillance activities on the trust in U.S. public cloud services. The second section will focus on the threat of economic espionage as perceived by the German companies. The last two sections will examine the opinions of the buyers and sellers regarding the actions and motivations of the U.S. government, German government and EU representatives in connection with the global surveillance activities.

6.2.4.1 Global surveillance disclosures

A key finding of the current research was that the global surveillance disclosures caused great uncertainty and concerns among German companies which had a negative impact on the public cloud computing adoption in Germany. The respondents of the German companies reported that they were shocked by both the intensity and extent of the revelations and that the NSA surveillance activities were the biggest scandal of the last years and led to a significant loss of trust. In a similar way, El-Gazzar (2016, p. 94) reported that companies in Norway stopped their cloud migration projects due to the Snowden leaks. For example, one Norwegian respondent said that “the project was stopped after all the headlines in the news with Edward Snowden

saying that the U.S. is reading mailboxes" and that they were "moving the mailboxes to another data server in Norway".

In the cloud computing literature, governmental influence was reported to have a negative impact on cloud computing services adoption (El-Gazzar, 2016). At the international level, laws and regulatory requirements make using multi-national cloud services complex (Marston et al., 2011). As described in Section 2.1.6, in the EU and in Germany there are serious concerns about data privacy, security and legal issues which raises several questions regarding accountabilities and responsibilities between cloud consumers and cloud providers (Seddon & Currie, 2013). This situation became even more complex after the global surveillance disclosures, which led to increased uncertainty (NTT, 2014; S. Schneider & Sunyaev, 2016). Likewise, S. Schneider and Sunyaev (2016) found that cloud computing services are characterized by a lack of transparency and uncertainty that hinder adoption. The authors gave the example of the "immature legal situation" between the U.S. and Europe and the global surveillance disclosures around the NSA PRISM programme.

Mistrust

In the wake of the global surveillance disclosures, German companies started to review their internal security and processes and took additional steps to protect their data from external access. To protect themselves against government spying, these companies therefore decided to keep their data either on-premise or only use data centres in countries that they considered safe. The mistrust in U.S. cloud services resulting from the global surveillance disclosures had probably a strong impact on the public cloud adoption of German companies.

As argued by Swan et al. (1988), mistrust takes time and effort on both sides, buyer and seller, to overcome. Moreover, mistrust "causes the buyer to take steps to protect his interests" (Swan et al., 1988, p. 2). Distrust is defined by Abdul-Rahman (2005, p. 47) as "to take an action as if the other agent is not trusted, with respect to a certain situation or context" whereas mistrust is defined as "a betrayal of the trust given by the trustee" (Huerta-Canepa, Lee, & Han, 2011, p. 470). The buyers of the current research argued that they could not trust someone who betrayed their trust before and reasoned that there was no guarantee that the U.S. government would not do this

again. Moreover, according to the respondents, it would take many years to rebuild the trust they lost in U.S. companies and the U.S. government.

This finding has important implications for U.S. cloud providers for developing long-term relationships with the German buyers. The statements of the buyer respondents suggest that it could be difficult for U.S. cloud providers to overcome the mistrust of the German customers. It might therefore take several years until the buyers of the German companies are willing to trust the promises of the U.S. cloud providers and the local sales representatives of the U.S. cloud providers would need perseverance, dedication and patience to build a trusting relationship with their clients.

Cloud adoption

As described in Section 2.3, cloud adoption in Germany was already low in comparison to other European countries or to the U.S. before the global surveillance disclosures. However, according to the respondents of the current research, the adoption slowed down even more after the Snowden revelations. This finding is in agreement with the findings of El-Gazzar (2016) which showed that the global surveillance disclosures caused an ongoing debate over the trust in U.S. cloud providers and whether companies should rely on local providers instead. Additionally, the present findings seem to be consistent with practitioner surveys on the matter. According to KPMG (2014), about 39% of the surveyed companies were “rather critical and refusing” towards cloud computing technologies. The authors of the study suggested that the “wiretapping practices” of government intelligence agencies would “certainly be an explanation” why the number of “cloud sceptics” was “still high” (KPMG, 2014, p. 7). Almost four-third of the respondents in the study of KPMG (2014) saw attacks by cyber criminals or intelligence agencies as a “real threat”. Furthermore, around half of the companies stated that their attitude towards cloud computing became more negative because of the NSA incidents. Respondents have also been asked what actions they have taken because of the “NSA espionage scandal” (KPMG, 2014, p. 31). Of the study population, 47% have either postponed or completely cancelled their cloud projects and 31% of all companies have “considerably increased their security requirements towards IT and telecommunications providers”. The authors of the study assumed that the NSA incidents will, at least in the short-to-medium term, be a burden for the development of the cloud market in Germany.

Interestingly, the concerns of their customers “over data access by investigatory authorities” was already a challenge for the cloud providers interviewed by PwC (2013a, p. 40) before the revelations of Edward Snowden and before the NSA surveillance practices have been reported in the press. Already then, three out of four cloud providers have been “often” or “occasionally” approached by their customers about the USA PATRIOT Act (PwC, 2013a, p. 39). The authors of the study of PwC (2013a, p. 39) explained that with the USA PATRIOT Act, “the powers of the American law enforcement agencies were significantly expanded” and that investigators from the USA could therefore “theoretically access data in the cloud at any time”. Accordingly, half of the clients of the cloud providers see the “possibility of authorities accessing data” as a “big problem” or even a “very big problem” (PwC, 2013a, p. 40).

In September 2013, after the first series of revelations by Edward Snowden, PwC (2013b) conducted an additional survey with 250 companies in Germany to specifically address this matter. PwC (2013b, p. 19) asked those companies how they assessed the “risk of fraud and abuse related to the use of cloud computing” and compared those results to the answers they received at the beginning of the year 2013, before the revelations Edward Snowden. It is apparent from Figure 17 that the number of companies that see a very high risk in cloud computing increased significantly after the revelations by Edward Snowden. The authors of the study concluded that, altogether, every second company (54%) saw a “high data security risk in cloud technologies” (PwC, 2013b, p. 19).

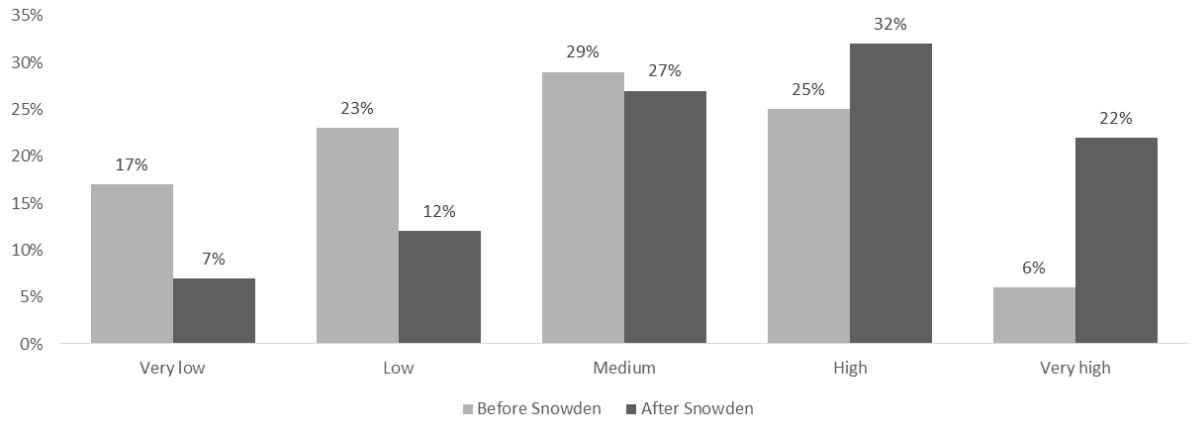


Figure 17: Cloud risks before and after Snowden. Adapted from PwC (2013b, p. 19).

Respondents have also been asked how they thought about “the use of cloud technologies in the light of the surveillance and espionage incidents” (PwC, 2013b, p. 20). Four out of five of the companies answered that they saw the usage of cloud technologies “rather critical” or “very critical” and only 2% of the respondents indicated that it was “rather uncritical” or “uncritical”. According to the authors of the study by PwC (2013b, p. 20), the results showed that the “already existing concerns about cloud technology” had been “reinforced after the incident”. Furthermore, almost one-fourth of the companies (24%) surveyed in the PwC (2013b) study answered that they see a higher risk of economic espionage after the press published the information they received from Edward Snowden. This concern of economic espionage in connection with the global surveillance disclosures will be discussed in the following section.

As discussed in Section 6.1.2.5, the German history makes Germans particularly sensitive to surveillance activities. The spying activities of the Nazi Secret State Police (GeStaPo) and the State Security of the GDR (StaSi) have an impact on the data privacy mindset of German citizens (Krasnova & Veltri, 2010). As stated by Lichter et al. (2016, p. 4), “the revelation of the NSA secrets affected ordinary peoples’ trust in the government” and “a substantial share of people stated that they adjusted their use of telecommunication as a consequence of the Snowden affair”. Hence, it could conceivably be hypothesised that the German history and culture had a strong impact on the cloud adoption in Germany and might explain why the surveillance activities of the U.S. government had potentially a stronger impact on cloud computing adoption in Germany than in other countries.

6.2.4.2 Economic espionage

Another important finding was the special significance of the threat of economic espionage for German companies in connection with U.S. cloud services. As described in Section 2.1.5.2, the German economy is particularly dependent on exports of high-tech products and many German SMEs are market leaders in their particular niche (Bryant, 2013c). Consequently, the protection of intellectual property and patents are of constant concern for German companies (Bryant, 2013b; Destatis, 2017). A characteristic of high-technology industries such as the automotive or chemical industries in Germany is that new technologies are constantly being developed which makes old technologies obsolete in a short period of time (Machin &

Van Reenen, 1998). The products that are based on these technologies are highly complex and require specialist knowledge to produce (C. J. Collins & Smith, 2006). As argued by Seppänen et al. (2007, p. 251), “technology and risks are often related, and therefore trust is a critical concept in technology-intensive industries”.

Several respondents used the term “fear” to describe their thoughts and feelings about economic espionage. This indicated that the notion of the “German Angst” discussed in Section 6.1.2 could also play an influential role when German companies are thinking of economic espionage in the context of public cloud computing. Additionally, the buyers argued that it was difficult for them to believe that the USA was only interested in terror prevention but might rather be interested in supporting the U.S. economy with foreign intelligence data. This supports the view of journalists, market research companies and politicians cited in Section 2.1.5.2 that German companies see economic espionage and the risk of intellectual property theft as a major challenge for cloud adoption. As described in the background chapter, Edward Snowden even mentioned the German company Siemens as one of the potential U.S. targets for economic espionage. The buyers claimed that the U.S. government would serve economic interests (e.g. in the oil industry) and it was therefore not unlikely that the U.S. government would also support their economy by sharing information gained from intelligence activities.

If U.S. intelligence agencies are actually involved in economic espionage activities, other U.S. companies than the U.S. cloud providers might benefit from the spying efforts and actively support certain political parties by lobbying and political donations. This would mean that U.S. cloud providers would not get much support by other U.S. companies in their efforts to limit the reach of U.S. intelligence agencies.

Knowledge protection

Norman (2002, p. 196) found that when companies face greater risk of knowledge appropriation by their business partners, “they will engage in behaviours to safeguard their knowledge”. However, the authors also found that “higher trust in a partner tends to reduce knowledge protection“ (Norman, 2002, p. 177). This indicates that a lack of trust in the U.S. cloud providers encourages German companies to protect their intellectual property by keeping their data on premise or selecting a European cloud provider.

The buyers explained that their companies decided not to save any confidential or business critical data at a U.S. cloud provider or any external provider. The seller respondents received similar feedback from their conversations with their German customers. This corresponds to a survey conducted by Corporate Trust (2014), which found that 22.5% of all economic espionage incidents in Germany occurred in the automotive, aircraft, ship and mechanical engineering industries. This underpins the assumption that the sector a company is operating in has a considerable impact on their trust in public cloud services. Several buyers and sellers of the current research stated that the manufacturing industry, the automotive sector and the automotive supplier industry were especially at risk of economic espionage. On the other hand, the IT manager of the advertising business explained that the risk of economic espionage related to public cloud computing was relatively low for his company.

According to a study by PwC (2014), 9% of the automotive companies in Germany became a victim of economic espionage in 2014. When asked about the types of sensitive data that should not leave the company, most of the German respondents (46%) answered that “research about new products” was not allowed to be stored outside the on-premise data centre (see Figure 18).

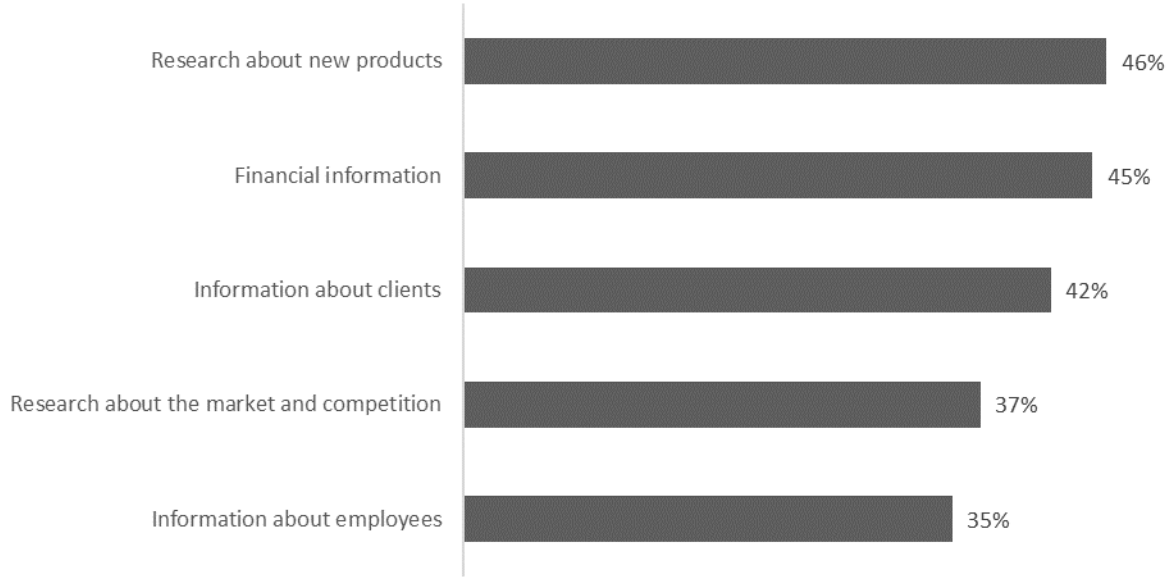


Figure 18: Types of data German companies keep on premises. Adapted from Mureșan (2016).

In contrast, IT decision makers from the U.S. and from the UK rated “information about clients” as the most sensitive data (Mureșan, 2016). This survey confirms that German

firms value intellectual property and research data higher than companies from other countries and that they are particularly concerned about someone stealing this information.

Value of data

According to economic thought leaders, “data is the new oil” (The Economist, 2017) and the current digitalization of all industries might lead to a situation where data is the most important and most valuable asset for many companies. This includes all kinds of data such as customer data, product data, production data, data from sensors of machinery and vehicles, research data and external data sources (Van der Aalst, 2014). Since more and more of their business depends on this data, companies have a high interest in protecting it from manipulation, deletion and theft (Nasheri & Blumstein, 2005). It is therefore understandable that companies are reluctant with giving their data to a third party such as a public cloud provider (Shackelford & Russell, 2014). On the other hand, to take advantage of the potential of their most valuable asset, their data, companies require the technologies offered by public cloud services such as data lake services, machine learning algorithms and global data replication capabilities (Miloslavskaya & Tolstoy, 2016). With the ongoing digitalisation of traditional businesses, it is not an option for most companies to ignore cloud computing technologies (Davis, Brodersen, Böhmer, & Siemens, 2017). In order to stay competitive and relevant, enterprises might therefore want to evaluate their individual business potentials and risks of adopting public cloud services and constantly monitor the fast-changing cloud computing market and adjust their specific business and IT strategies accordingly.

The findings of the current research suggested that the fear of German companies of economic espionage played a significant role in the opposition to U.S. public cloud services. However, the current research was not specifically designed to evaluate this factor in detail. Further research regarding the role of economic espionage in connection with the trust of public cloud services would therefore be worthwhile. Additionally, a further study could assess if this attitude is specific to the German market or if other countries with a similar dependence on exporting high-technology goods such as machinery and chemicals share these fears.

6.2.4.3 U.S. government reactions

Both buyers and sellers agreed that they lost their trust in the U.S. government and that it was unlikely that the U.S. government would make any substantial changes to the surveillance law anytime soon. This confirms the analysis in Section 2.3.1 that the U.S. government did not share the concerns of the European countries and that the measures that were announced by government officials were vague and half-hearted. Kshetri (2013) studied the role of institutions regarding privacy and security issues in cloud computing and named national governments as a key institutional actor associated with the cloud industry. He gave some examples of government actions which included the FISMA in the U.S., the legislations governing the location of storage for personal and medical data in the U.S. and UK and European privacy laws. Although Kshetri (2013, p. 5) published the study prior to the Snowden revelations, he already argued that “some governments are using the coercive power of the state to use the cloud in spying on citizens”. As discussed in the previous section on economic espionage, this was also one of the allegations made by the German companies against the U.S. government.

Kshetri (2013) speculated that governments were likely to face pressures to strengthen cloud-related legal system and enforcement mechanisms and to harmonize and align their legal systems and enforcement mechanisms with those of other countries. Similarly, J. Smith and Wiest (2005) predicted hat national governments were increasingly turning to supra-national institutions to resolve transnational problems with the alignment of legal systems. A few sellers argued that the U.S. government would not change anything without the pressure of the U.S. technology sector. However, with exception of the EU, legislation around data privacy and cloud computing services is still a national domain and international agreements are rare (Cheung & Weber, 2015; Jaeger et al., 2008; Millard, 2013).

Recent developments

The respondents were rather sceptical of the reactions of the U.S. governments after the global surveillance disclosures. They asserted that the U.S. government only made a public statement after they could no longer hide and that they have not made any substantial changes. Some of the buyers argued that they would wait until a new legislation was in place to prevent further surveillance activities. However, five years

later, it is still controversial if the Snowden's disclosures caused any substantial political and institutional changes (S. Gallagher, 2018).

A recent development that happened in the time after the interviews and data analysis of the current research was a change of the presidency of the U.S., as well as a change of the governing party of the country. This poses the question how the new president and his politics will influence the trust of German companies in his government bodies and cloud services provided by U.S. companies. The key slogan of his campaign “America first” (Rothman, 2016) and his announcements to date suggest that the government influence on U.S. companies including cloud providers might not decrease. International privacy and human rights activists expressed fears over the prospect of President Donald Trump controlling the U.S. intelligent agencies and surveillance networks (Ackerman & MacAskill, 2016). They expected the balance between surveillance and privacy to tip towards mass surveillance activities. As one of his first actions, in April 2017, Donald Trump signed a law allowing U.S. internet companies to sell the internet browsing histories of their customers (Griffin, 2017). German news agencies are already warning that because of the new U.S. government, transferring data to the U.S. can be risky (Heidrich, 2017) and are recommending to German citizens to keep their data in the EU (Bager, 2017).

Already in February 2017, U.S. technology companies and cloud providers spoke out against President Donald Trump’s immigration policy (Sherr, 2017) and supported a lawsuit against the executive order of the president (Etherington, 2017). One month later, in March 2017, leading U.S. technology companies announced that they will not support the executive order of President Donald Trump supporting gas and coal power plants but continue their support for renewable energy (Murray, 2017). According to Mateo Meier, founder of the cloud provider Artmotion, the U.S. cloud computing industry could lose more than $10 billion by 2020 as a result of President Trump’s reputation on data privacy (Ismail, 2017). In 2018, President Donald Trump renewed attacks against U.S. technology companies, for example by accusing Google’s search engine of promoting negative news articles and hiding “fair media” coverage of him (Holland & Mason, 2018; Reuters, 2008). The U.S. press also reported about several attacks on the online retailer and cloud provider Amazon (Davies, 2019; Helmore, 2018; Sherman, 2018). Another contentious issue is the discussion around trade tariffs

between the U.S. and China (Berniker, 2018). U.S. technology companies warned that China tariffs can hurt their business and their customers (Mayeda, 2018; Rappeport, 2018). In December 2019, Amazon sued the U.S. Department of Defense, claiming that the president's “highly public personal vendetta against Mr. Bezos, Amazon, and the Washington Post” pushed Pentagon officials to award a $10bn cloud-computing services contract to rival Microsoft (Ivanova, 2019, p. 1).

These developments suggest that the upcoming years might be turbulent times for cloud providers and their potential customers, and that this uncertainty will probably not help rebuilding trust in U.S. cloud services.

6.2.4.4 German and EU government reactions

From the point of view of the respondents of the current research, the words and actions of the German and EU politicians as outlined in Section 2.3.1 did not produce the desired results of protecting the German and EU citizens from surveillance activities and re-establishing trust in their government. The answers of the interviewees suggest that the buyers and sellers were frustrated about the lack of action by German and EU politicians. These results would seem to suggest that the global surveillance disclosures not only damagingly affected the trust of German companies in the U.S. government but also in their own national and EU institutions. The respondents urged the German government to exert pressure on the U.S. government.

As reported in Section 2.3.1, in 2012, the European Commission published a paper titled “Unleashing the Potential of Cloud Computing in Europe” to promote cloud computing in the EU by introducing common standards, fair contract terms, and a European Cloud Partnership (ECP) (European Commission, 2012d). to build a new industry and “better competing against the United States in particular” (European Commission, 2012e, p. 2) to “become a world cloud computing powerhouse” (European Commission, 2012d, p. 16). In 2013, after the Snowden revelations, European Commissioner for Digital Agenda, Neelie Kroes, stated that privacy could be used as a competitive advantage by European cloud providers (European Commission, 2013f, p. 2). Kshetri (2013, p. 12) argued that, “given the cloud’s significance to economic competitiveness and national security, policy makers need to look at developments in cloud-related institutions in other countries and take

proactive measures to enact and enforce laws for developing the cloud industry". This view was also shared by the respondents of the current research. The buyers stated that companies such as Siemens were once manufacturers of semiconductors, computers and mobile phones but that they sold those assets and withdrew from the information technology sector. They demanded that the German government should make investments in German technology start-up companies and create incentives for technology companies to create jobs in Germany.

Technological knowledge

However, at the same time, the respondents did not have confidence that the German government would have the necessary knowledge, skills or intentions to increase the competitiveness of the German information technology sector. This view is also shared by privacy advocates and journalists reporting on technology and privacy topics. A recent example is the testimony of Facebook CEO Mark Zuckerberg to the United States Senate Committee on Commerce, Science, and Transportation on the 10th and 11th of April 2018 regarding the usage of personal data by Facebook in relation to the Facebook–Cambridge Analytica data breach (U.S., 2018b). As a response to the public hearing the press and privacy advocates reported that "relatively few US senators understand Facebook's business" (Tibken, 2018, p. 1), that "Washington doesn't understand technology" (Pring-Mill, 2018, p. 1), that "lawmakers seem confused about what Facebook does" (Stewart, 2018, p. 1) and that "politicians are too out of touch to make laws about tech" (Cawley, 2018b, p. 1). Another example is the rearing of Sundar Pichai, Google CEO on the 11th of December 2018 where the press reported that "Congress missed another chance to hold big tech accountable" (Newton, 2018, p. 1), which "further demonstrated the growing knowledge gap between tech and politics" (Cawley, 2018a, p. 1) and was called another "reminder of Congress's continued technological ignorance" (Lapowsky, 2018, p. 2). This criticisms regarding a lack of information technology knowledge is not only directed at U.S. but also at European politicians (Brühl, 2018; C. Lee, 2016).

In general, citizens' trust in government has declined over the last years (Citrin & Stoker, 2018; Enli & Rosenberg, 2018). One reason for this decline were political scandals that destroyed the trust in the politicians. As demonstrated by Bowler and Karp (2004), political scandals can have a negative influence on citizen's attitudes

towards politicians, institutions and the political process. Rothstein and Stolle (2008, p. 34) argued that “trust thrives most in societies with effective, impartial and fair street-level bureaucracies” whereas König and Schuknecht (2018) found that public’s trust in the government strongly depends on governments delivering on their core tasks.

GDPR

The buyer respondents of the current research required clear guidance and privacy protection from politicians and the sellers wished that the governments of the EU countries and the U.S. would come to an agreement. Despite some criticisms related to the reactions of EU and German government officials, there might be one key element of today’s EU data privacy policy that might have not existed without the global surveillance disclosures. According to political scientists, Snowden’s revelations inverted the direction of the European Parliament’s debate on the General Data Protection Regulation (GDPR) (Phillips, 2018). They argue that, before the global surveillance disclosures, the privacy rules of the EU were mainly shaped by corporations (Rossi, 2018). However, after Snowden’s revelations, the power of corporations regarding privacy politics decreased and privacy advocates were able to shape the content of the GDPR (Berg, 2018; Schallbruch & Skierka, 2018). According to Jan Philipp Albrecht, one of the authors of the GDRP, the Snowden revelations helped to unite the European interests and come to a common agreement (Tatje, 2013). Therefore, the revelations by Edward Snowden were instrumental in defeating corporate power and enabling Europe’s privacy advocates to make the European Parliament agree on a common European privacy standard (Goldsmith, 2018).

However, the global surveillance disclosures were not the only data scandal in recent years. For example, in March 2018, whistle-blower Christopher Wylie revealed that data analytics firm Cambridge Analytica that worked with Donald Trump’s election team and the winning Brexit campaign harvested about 50 million Facebook profiles in a major data breach (Cadwalladr & Graham-Harrison, 2018). Therefore, it cannot be ruled out that there will be additional data privacy incidents in the future and that policy makers need to further adjust the current legislation to the everchanging threats.

6.2.4.5 Summary

The findings discussed above provide some support for the conceptual premise that the foreign government trust relationship has the strongest impact on the purchase decision of the buyer. The findings from the interviews match those observed in earlier studies that the global surveillance disclosures caused mistrust in U.S. cloud providers and slowed down cloud adoption in Germany. A key element was the fear of economic espionage and the subsequent protection of company data and intellectual property. As a consequence, German companies are more likely to spend time and money on monitoring foreign government activities and protecting their data from external access instead of investing in international business partnerships with U.S. cloud providers.

The respondents made it clear that they did not have any trust in the U.S. government which could not be compensated by the reactions of the U.S. cloud providers. Recent developments in U.S. politics might not have improved the critical attitude towards U.S. government organisations or might have even worsen it. Moreover, the interviewees also maintained that they could not count on the German or EU governments to defeat the surveillance threat. In accordance with the present results, previous studies have demonstrated that politicians lack technological knowledge and might therefore not be able to make the right decisions to prevent foreign surveillance activities and economic espionage in public cloud services.

It might therefore be the case that the distrust of the buyers in the foreign government overruled the trust relationship in the company, product and salesperson and that these three relationships do not have much impact on the purchase decision of the buyer as long as the buyer does not have trust in the foreign government. However, as argued by Fang et al. (2008), it is critical to the success of buyer-seller collaboration to build and manage trust at multiple levels. It could therefore be argued that the relationship between the buyer and the selling company, between the buyer and the product, between the buyer and the salesperson and between the buyer and the foreign government all play a non-negligible role.

6.3 How U.S. cloud providers can improve the trust relationship (RO3)

The third objective of the current research was to identify ways how U.S. cloud providers can improve the trust relationship with German companies. The following sections will address the managerial implication of this buyer-seller trust relationship

by discussing the four most frequent answers of the research respondents to the question how U.S. cloud providers can win back their trust. As concluded by Schurr and Ozanne (1985), high trust causes a more favourable attitude toward the seller and a more favourable attitude toward loyalty than low trust. Therefore, U.S. cloud providers should have a strong interest in improving the trust of their potential customers in their products/services, company and salespeople.

6.3.1 Data centre location

As explained by some of the buyers and sellers, for most businesses in Germany, there is no legal difference between a data centre in Germany and a data centre in another EU country such as Ireland. However, as stated by the respondents, the data centre location is one of the key topics in their discussions with German companies. As argued by Jon M. Hawes et al. (1989), “the reality of how much risk is present in a potential exchange is not as critical as the potential buyer's perception of this risk”. Therefore, even if a German data centre does not reduce any risk for the buyer in comparison to a data centre in Ireland, the buyer’s perception of the situation and the attendant attribution of trust to the cloud provider might lead to a business relationship between the parties.

There are similarities between the attitudes expressed by the buyers in this study and those described market research companies. An earlier study conducted by Deloitte (2011) revealed that German businesses consider the location of the provider and its data centres as an important aspect when making their decision for the right cloud provider. The vast majority of the companies surveyed by KPMG (2014, p. 33) demanded that the cloud provider has to have its headquarters in Germany (77%) or at least in the EU (73%). This result was also reflected by the question if the companies would prefer a “national cloud”, where only 35% of the respondents did not prefer this option. The study concluded that it was therefore “beneficial for cloud providers” to have data centres in Germany respectively in the EU (KPMG, 2014, p. 36). These results agree with the findings of other studies. According to a survey by NTT (2014, p. 3), almost one third of the IT decision makers of German and U.S. companies “agreed that location completely matters when thinking about data storage in the cloud”.

In a more recent survey conducted by iSense Solutions with 503 IT security purchase professionals, 89% of the German respondents stated that they preferred to keep their data in Germany (Mureșan, 2016). As shown in Figure 19, only 5% of the respondents trusted the U.S. with their data.

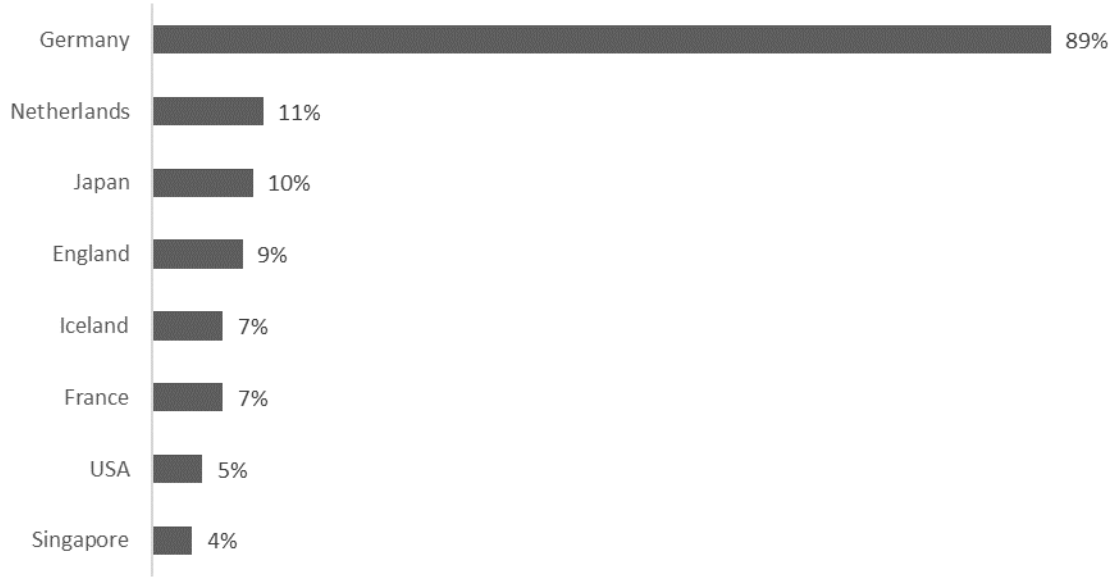


Figure 19: Location of most-trusted cloud computing providers. Adapted from Mureșan (2016).

Moreover, when asked about the "location of the least-trusted cloud computing service providers", most of the German respondents (54%) named the U.S. as the least trustworthy country, even before India and Singapore (see Figure 20).

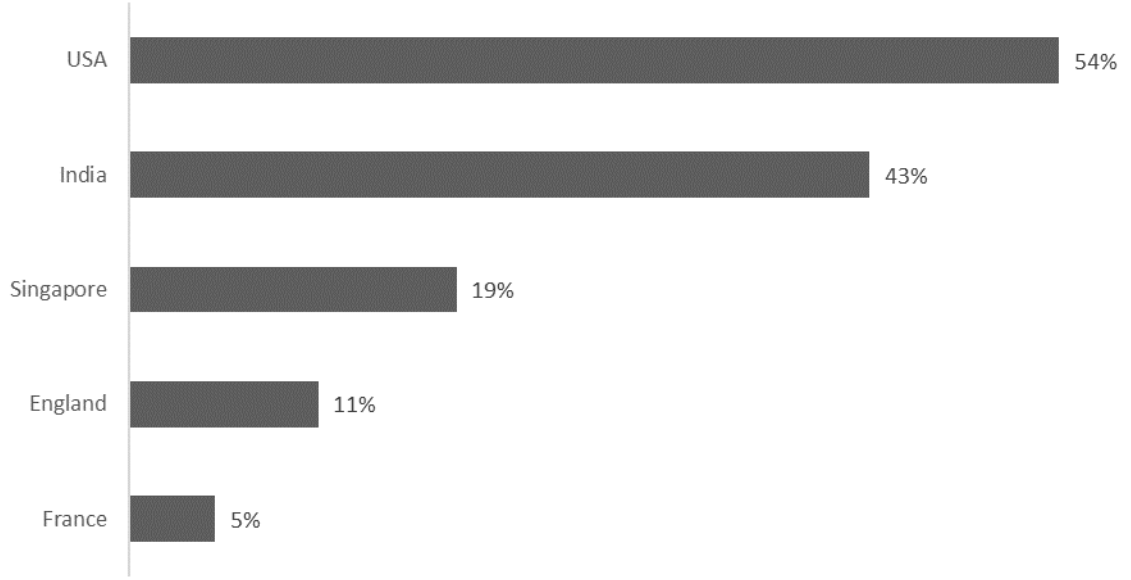


Figure 20: Location of least-trusted cloud computing providers. Adapted from Mureșan (2016).

As described in Section 2.3.3, U.S. cloud providers already reacted to the NSA surveillance disclosures and changed their market strategy. One consideration was the location of their data centres (Boulton, 2016; Scott, 2016). During this research, several U.S. cloud providers have announced that they would build local data centres in Germany. This shows that the statements of the interviewees of this study correspond with the actual needs of German companies and that U.S. cloud providers are already acting to win back the trust of their customers in Germany.

In October 2014, Amazon (2014) opened a new data centre region in Frankfurt, Germany for their Amazon Web Services (AWS) customers in Europe. They did, however, not guarantee that the U.S. government would not have access to the data stored in their German data centres (The Register, 2014). A few months later, in January 2015, as part of its $1.2 billion investment to expand its global cloud footprint, IBM (2015) announced the opening of its first cloud data centre with SoftLayer in Frankfurt, Germany. Other U.S. cloud providers followed. VMware (2015) opened a data centre in Frankfurt, Germany in March 2015 and Salesforce (2015) opened their local data centre in Germany in August 2015 in cooperation with T-Systems.

Later that year, in November 2015, Microsoft (2015) announced plans to offer cloud services from German data centres. Microsoft proclaimed that their employees would not get access to any data stored in the German data centres (Büst, 2015). The

German telecommunications and IT provider T-Systems, a subsidiary of Deutsche Telekom, controls and oversees all access to customer data. According to industry experts, this construct allows Microsoft to protect the data of their European customers from access by the U.S. government through National Security Letters (Moody, 2015). In February 2016, Dropbox (2016a, 2016b) reported that they would allow their customers to store their files in a data centre in Germany through a cooperation with Amazon Web Services (AWS).

However, the demand of German companies for more transparency about how U.S. cloud providers are running their data centres could also turn into a security issue. The question arises of how much transparency is enough. As suggested by Michael (2009, p. 3), there might be a tipping point at which additional transparency might not improve trust but might "only serve to help malefactors compromise the services and data centres". U.S. cloud providers therefore need to carefully decide what information about the data centre infrastructure and proceedings are safe to communicate to external parties.

This finding has important implications for developing cloud service offerings for German companies. One of the issues that emerges from these findings is that German companies prefer to save their company data in Germany and avoid saving any data in U.S. data centres. In general, therefore, it seems that the current investments of U.S. cloud providers in local data centres in Germany are a step in the right direction to win back customer trust. However, more research on this topic needs to be undertaken before the association between local data retention and customer trust is more clearly understood.

6.3.2 Legal proceedings

On the question of how U.S. cloud providers could improve the trust with German companies, this study found that filing an action against the U.S. government regarding the practices of the U.S. intelligent agencies might contribute to restoring trust of the buyers. Some of the buyers stated that this approach might build trust since potential cloud consumers would see that the U.S. cloud providers would be on their side. However, not all buyers were convinced that the U.S. cloud providers would take a side against the U.S. government. They explained that this was a step in the right direction but that they could not tell if the legal actions against the U.S. government

were meant to protect their customers or if they were part of a marketing initiative. All cloud sellers agreed that it was important for their business that the U.S. cloud providers would adopt a position clearly and roundly condemning the eavesdropping practices of U.S. intelligence agencies by taking legal measures following these incidents.

Over the course of this research, several U.S. cloud providers acknowledged that there was a need to defend themselves against the activities of the U.S. intelligent agencies and to make their disputes with the U.S. government public. As described in Section 2.3.3, some of the most prominent U.S. technology companies joined forces and wrote collective letters to U.S. government officials and asked for changes to the prevailing legal situation. Moreover, the responses of the U.S. cloud providers also included legal actions. For example, in December 2013, Microsoft denied to hand over emails to the U.S. government that were stored on servers located in Dublin, Ireland (CDT, 2014). In April 2014, a U.S. magistrate judge denied Microsoft's motion to quash the warrant. Backed by the Irish government and several U.S. companies, Microsoft decided to appeal against the court decision (Scott, 2014b). In July 2016, the United States Court of Appeals for the Second Circuit reversed the ruling of the lower court (Wingfield & Kang, 2016). The Circuit judge advised the U.S. Congress to modernise the "badly outdated" law to achieve a better balance between privacy interests and law enforcement needs (Stempel, 2016, p. 2). In October 2016, the U.S. Justice Department asked the full appeals court for the Southern District of New York to review the decision (Nakashima, 2016). However, in January 2017, the federal appeals court decided against reviewing a decision forbidding the U.S. government from forcing Microsoft to turn over customer emails stored on servers in Ireland (Stempel, 2017).

In June 2017, the U.S. Department of Justice, joined by 33 states in support (Stohr, 2017), filed an appeal with the U.S. Supreme Court and the case was heard by the Court on the 27th of February 2018 (Kravets, 2017). Shortly after the oral hearings, the U.S. congress introduced the Clarifying Lawful Overseas Use of Data Act ("CLOUD Act") (U.S., 2018a) which was supported by both the U.S. Department of Justice and Microsoft (Breland, 2017). The CLOUD Act modified the Stored Communications Act of 1986 to include cloud storage considerations of communication providers in the U.S. regardless of where the cloud servers are located. After the U.S. congress passed the

CLOUD Act, the U.S. Department of Justice issued a request for a new warrant for the original emails (Stohr, 2018) and requested that the U.S. Supreme Court rendered the case moot (Nakashima, 2018). Microsoft agreed with the position of the U.S. Department of Justice and called for dismissal of the dispute (Hurley, 2018). However, according to Microsoft's chief legal officer Brad B. Smith (2018), the CLOUD Act was only a first step in the journey to modernise privacy laws.

The fact that U.S. cloud providers started to take legal actions against the U.S. government could be considered as a confirmation that the requests of the respondents of the current research match the wishes of other customers who expressed their discontent to the U.S. cloud providers. Therefore, the present findings seem to be consistent with other customer statements and emphasize the importance of legal measures for the trust development process by U.S. cloud providers.

6.3.3 Cloud computing contracts

Another legal topic was the form and content of cloud computing contracts. As shown in the findings, the respondents of the German companies sharply criticise the contractual frameworks for cloud services with U.S. cloud providers. They explained that the majority of the current contractual templates for U.S. cloud services were based on a jurisdiction in the U.S., England or Ireland and argued that German companies should get the option for a contract based on German law. Moreover, the contracts were described as being too complex. Some of the buyers argued that even their own lawyers would not completely understand the contractual content and that they would require external consultancy to cover these topics. However, as maintained by Rohrmann, Cunha, and Falci (2015, p. 45), it was essential that "the legal department of large companies are technically prepared to negotiate and enter into comprehensive contracts providing cloud computing". The authors found that it was necessary to properly understand the cloud computing services and deployment models (as explained in the background chapter) as well as the various cloud solutions available. In the case of cloud computing contracts, "standards are generally detailed in an SLA or attached schedules" (Gleeson & Walden, 2014, p. 18). Since cloud computing provides several services for critical business applications, SLA are very important in cloud computing business agreements (Mirobi & Arockiam, 2015). It could therefore be argued that not only U.S. cloud providers need to adapt their contracts to

the European and German market, but German companies and their legal advisors also need to get a better understanding of cloud computing services in general and the legal specifics in particular.

A further criticism made was that the U.S. cloud providers were not willing to make amendments to the original contracts but required the German companies to sign the contract without suggesting any changes. The request from the German companies was that terms and conditions of cloud contracts should be mostly identical their on-premise infrastructure contracts. In their opinion, U.S. cloud providers would be more successful on the German market if they would listen to the needs of their German customers and changes their contractual language accordingly. The findings of the current study are consistent with those of Hon, Millard, and Walden (2012, p. 126) who found that, in order to stay competitive, cloud providers have to be more aware of the concerns of their users as well as being “more flexible in negotiations” and more willing to modify their contracts to meet the requirements of their customers in terms of security, privacy and legal requirements. Similarly, Bradshaw, Millard, and Walden (2011, p. 46), argued that once customers experience that some cloud providers start to offer terms and conditions that “offer more in the way of enforceable rights than others do”, the presence of these rights might become a competitive advantage. Rohrmann et al. (2015) concluded that cloud computing contracts should meet the interests of both parties and should not only include the typical SLA in terms of security, integrity and reliability but also “issues regarding intellectual property and data encryption”. This is in line with the findings of the current research, where the key informants highlighted their concerns regarding economic espionage (see Section 6.2.4.2) and the need for strong data encryption services as discussed in the following section. Rohrmann et al. (2015) further recommended that it was important to create cloud computing contracts where the duties and obligations of both parties are clearly understood to avoid problems such as losing sensitive information to competitors. In a study on the relationship between contracts and trust, Woolthuis, Hillebrand, and Nooteboom (2005, p. 835) found that contracts and trust need not be “opposing alternatives” and that they can “well be complements”. Therefore, contracts and trust between buyers and sellers need to have the right balance in order to have a positive impact on the business relationship between the parties.

However, not all respondents believed that better contracts would improve trust. Some of the buyers argued that the contractual agreements between them and the U.S. cloud providers would not create trust until the U.S. would change the legal frameworks allowing U.S. intelligence agencies to request U.S. cloud providers to hand over customer data. As discussed in Section 6.2.2, the trust in the U.S. cloud provider company was displaced by the distrust in the U.S. government since the U.S. cloud providers could not guarantee that the U.S. government would not get access to customer information. Therefore, the risk of storing their data with a U.S. cloud provider outweighed the technological and financial benefits that U.S. cloud providers might offer. This statement can therefore be seen as another example that the NSA surveillance activities had a strong negative impact on the trust of German companies in U.S. cloud provider companies and that U.S. cloud providers had to actively work on measures to win back the trust of German businesses.

The cloud sellers agreed with the buyers that U.S. cloud providers should modify their standard contracts to meet the requirements of German companies. They confirmed that customers demanded contracts in accordance with German law with a place of general jurisdiction in Germany. These results match those observed in earlier studies. For example, T. N. Foster (2013) found that cloud computing contracts are unevenly balanced in the favour of cloud computing providers and recommended that additional legal and practical measures are necessary to achieve a reasonable level of data privacy, security and confidentiality. Similarly, Mualla and Jenkins (2015) concluded that most cloud computing contracts would only include limited guarantee on service quality assurance and that business would therefore be reluctant to outsource any business critical infrastructure to public cloud services.

Additionally, the cloud sellers reported that their customers would require the local sales representatives of the U.S. cloud providers to be familiar with the European and German laws and regulations and to assist their German customers in being compliant when using U.S. cloud services. The cloud sellers stated that contracts should be in German language and argued that the U.S. cloud providers would underestimate the needs of German companies regarding security and compliance. As stated by the cloud sellers, the European and German law requires U.S. cloud providers to adjust their standard contracts. This was probably the intention of a working group

established by the European Union. On 18 June 2013, the European Commission (2013a) set up an expert group on cloud computing contracts to assist the European Commission in identifying safe and fair contract terms and conditions for cloud computing services for consumers and small firms. The task of the group was to use existing best market practices in terms and conditions in cloud computing contracts and the protection of personal data. The work of the expert group provided input to several directive proposals to the European Parliament. As reported in Section 2.1.6.3, U.S. cloud providers already made several modifications to their contracts and services during the time after the interviews including the compliance with the EU's General Data Protection Regulation (GDPR). This confirms the validity of the requests and recommendations by the buyers and sellers of the current research regarding the modification of the contractual framework of the U.S. cloud providers.

Moreover, this provides additional evidence to the findings discussed in Section 6.2.3 that the salespeople of the U.S. cloud providers not only require knowledge and expertise of their products and services but also of the characteristics of the German market and the sector or industry the German company is operating in.

6.3.4 Data encryption

An additional recommendation expressed by the key informants was the encryption of data. As reported in the findings chapter, the buyers were particularly interested in using their own encryption keys in a "bring you own key" scenario. Cloud computing data can be encrypted "in transit" and/or "at rest" using key management services and a variety of encryption algorithms (Li, Li, Chen, Jia, & Lou, 2015; Priyam, 2018). In case that the data owner encrypts the data, the cloud provider does not get access to the information stored in the cloud data centre (Patil, Khatawkar, & Dange, 2017). The present findings seem to be consistent with previous research. As found by Jayapandian, Rahman, Sangavee, and Divya (2016), client side data encryption can increase cloud security trust and drive cloud adoption. The authors of the study of PwC (2013a, p. 43) concluded that "customer interest in data privacy measures increased significantly" in the last years which shows that cloud providers need to proactively address this matter in order to win customers in Germany. The two main information security aspects of the customers of the cloud providers were that adjustments of security concepts should be based on customer requirements (90%) and the

encryption of customer data (87%). However, not all respondents agreed that data encryption would improve trust in public cloud services. Moreover, a few buyers pointed out that since data was an intangible good, it was difficult or even impossible to find out if data was stolen from a public cloud provider. It could, however, be argued that the same could be said about data stored in the private data centre of the German companies and that encrypting their data would help protecting their assets in case of data theft.

From the point of view of the cloud sellers, data encryption was a regular topic in their conversations with German customers. As described in Section 2.3.3, some cloud providers such as Google already invested in additional encryption technologies as a response to the global surveillance disclosures. Other providers such as Amazon (2016), Microsoft (2016) and Salesforce (2016) also started to offer “bring your own key” (BYOK) solutions where customers can use their own encryption keys to secure their data. This approach requires that companies invest in trainings and develop sophisticated key management procedures because operating errors could potentially lock out the customers from their own data.

Though, the local sales representatives of the U.S. cloud providers also warned of the negative effects of data encryption and pointed out that the use of data encryption would also create new challenges for cloud consumers and cloud providers. For example, end-to-end encryption could possibly prevent some cloud services, such as indexing and search, from working as intended. This, however, contradicts many of the reasons why companies are adopting cloud services, such as simplicity, speed and cost savings (Branscombe, 2015). Overall, these results indicate that data encryption technologies could be a way to build a secure environment for customer data in the cloud. However, some cloud functionalities might not work as well as with non-encrypted files and it requires additional effort to maintain this solution. Therefore, public cloud providers are constantly working on ways to improve the customer experience with data encryption and adding new encryption technologies such as computing on encrypted data (Agrawal, Agrawal, & Prabhakaran, 2015; Freris & Patrinos, 2016; Fu, Sun, Liu, Zhou, & Shu, 2015). For example, Microsoft introduced Azure confidential computing (Russinovich, 2017) Google created Asylo, an open source framework for confidential computing (N. Porter, Garms, & Simakov, 2018).

Overall, it is striking that all four recommendations discussed above are aiming to improve or obviate the need for the trust in the foreign government. The location of a data centre in Germany forces foreign governments to ask for administrative assistance of the German government, so called mutual legal assistance treaties (MLATs), if they need access to data stored in Germany (W. Maxwell & Wolf, 2012, 2013). The legal proceedings of U.S. cloud providers against the U.S. government makes requests for data handover to U.S. government agencies public and prevents unlawful activities. A place of jurisdiction in Germany ensures that German and European law is applied and that German companies are in full compliance with the existing legislative framework. And strong data encryption mitigates the risks of wiretapping of foreign intelligence agencies and cooperation between cloud providers and foreign governments. This can be interpreted as a further indication that the trust of the buyer in the foreign government has a greater influence on the purchase behaviour than the trust in the company, product/service or salesperson. It would therefore be in the best interest of the U.S. cloud providers to make encryption technologies more accessible for their customers and educate their clients on how to manage the complexity of cloud data encryption.

6.4 Conceptual framework (RO4)

The fourth objective of the current research (RO4) was to develop a conceptual framework for buyer-seller trust in the context of international public cloud computing services. The framework (see Figure 21) summarizes some of the findings and ideas developed in the current research and makes a contribution to knowledge as well as to practice. The concepts are based on the results of the current research in the context of the trust between German companies and U.S. cloud providers and might not be applicable to other settings or generalizable for other industries.

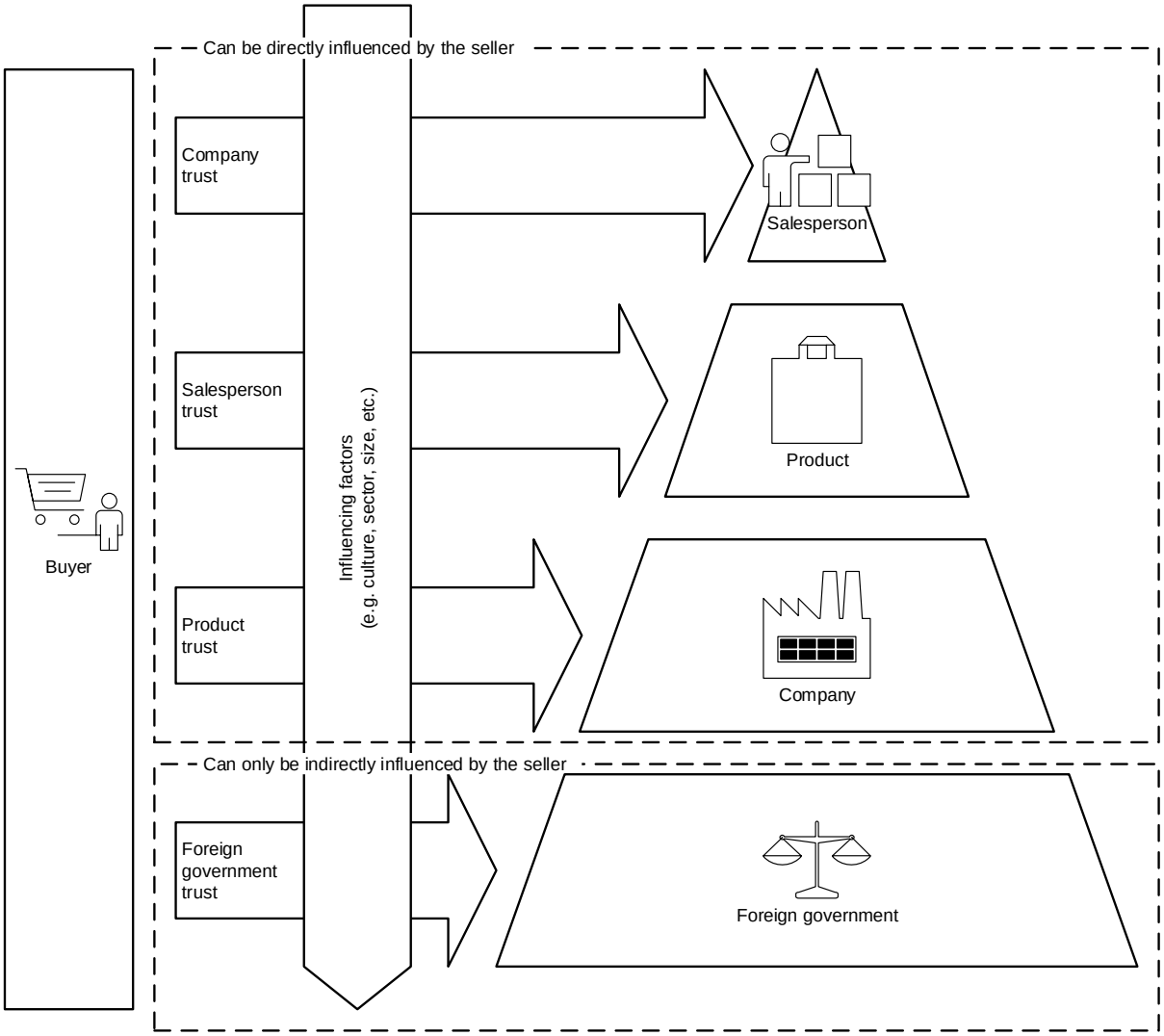


Figure 21: Conceptual framework

Firstly, the conceptual framework shows the impact of the different trust relationships on the buyer's purchasing behaviour. One of the key findings of the current research was that the **trust in the foreign government** might be able to overrule the trust relationship in the company, product and salesperson. Figure 21 shows a hierarchical order of the four trust relationships in which foreign government trust can be seen as the foundation. The next level is the trust in the company, which is often represented by a brand and has a direct influence on the trust in the product or service of the company. As several respondents reported, their distrust in a company led them to avoid all products and services of that company. The trust in the salesperson is the least important level. As discussed earlier, with public cloud computing services, buyers can make a purchase directly from the website of the cloud provider company and are not required to talk to any salesperson. Several interviewees stated that a

local salesperson was not important for their purchase decision and the more cloud services will become commoditized, the more they will be bought directly from the provider's web portals. However, the present findings seem to be inconsistent with previous research which found that salesperson trust was as important or even more important than the other trust relationships. Similar to the hierarchy of needs by Maslow (1943), the trust in the lower parts of the pyramid must be present before the buyer will focus on the higher levels.

Secondly, the framework illustrates that all four trust relationships are influenced by external factors such as the **cultural background** of the buyer and seller and the **sector and size** of the buying company. For example, as discussed in Section 6.1, the degree of the objection against government surveillance activities is subject to the individual cultural background, and the fear of shadow IT and economic espionage are to a great extent dependent on the sector a company is operating in. As discussed in Section 6.1.2, the cultural background can have a strong influence on the decision-making process of buyers. Depending on these external factors, the trust relationships of the buyer and the salesperson, product/service, company and foreign government are perceived and weighted differently by the buyer. For instance, a buyer from the insurance sector has different priorities and different boundary conditions from a buyer in the media industry. The trust relationships are also subject to additional external factors which could be addressed in future research. This could for example be the technical knowledge and openness of the decision makers or the company's business strategy and financial situation.

And thirdly, the framework suggests that the traditional trust relationships (company, salesperson, product/service) can be **directly** influenced by the seller, whereas the trust relationship between the buyer and the foreign government can only be **indirectly** influenced by the seller. As discussed above, all measures suggested by the German companies on how U.S. cloud providers can improve the trust relationship with German companies are aiming at improving or obviating the need for the trust in the foreign government. However, these actions only mitigate the risks of negative effects of foreign government policies on the buyer. The sellers do not have any direct influence on the decisions of the foreign government and need to adjust the measures to improve the buyer's trust every time the government changes its course or by

lobbying activities that might be costly and lengthy. The other trust relationships, in turn, can be directly influenced by the seller by, for example, changing the company's marketing strategy, improving the quality of the product or hiring/training the company's salespeople. Foreign government influence on the selling company, the product/service or the salesperson induced by legislation and executive forces are not specifically highlighted in the framework since this was not specifically addressed by the objectives of the current research. However, as discussed above, the foreign government might have direct influence on the actions of the selling companies through an administrative subpoena and thus on the corresponding salespeople and products/services.

This conceptual framework also contributes to practice. It can help cloud providers to improve the trust relationship with their potential customers by systematically identifying potential sources for distrust and prioritising the measures to improve customer trust. In order to win and maintain the trust of their customers, sellers need to take these factors into account and adjust their sales approach accordingly. It could be argued that the dependency on the national and international politics of the government implies incalculable risks for the buyer and for the seller. This means that the buyer should be well informed about the juristic and practical reach of the foreign government and select their business partners accordingly. The seller, on the other hand, should consequently take the perspective of the buyer to find potential barriers that are stopping them from purchasing their products or services. However, the seller may only have limited influence on government legislation and activities.

Therefore, the trust of the buyer in the foreign government can be described as volatile since government policies and actions are subject to constant changes and are not predictable by the buyer or by the selling company. Accordingly, buyers should be aware of the possibility that a change in the political situation can have an impact on running contracts with their cloud providers. However, the more data and business applications are moved to a public cloud, the more complex, time-consuming and expensive is a migration to a different provider or back to on-premise server systems can be. This so-called vendor lock-in could therefore become a significant risk for the buyer if a fast exit becomes necessary because of potential foreign government policy changes.

7 Conclusions

The last chapter of this thesis is divided into three parts (see Figure 22). The first section outlines how this work contributes to existing knowledge. The second section will highlight the practical applications of the current research.

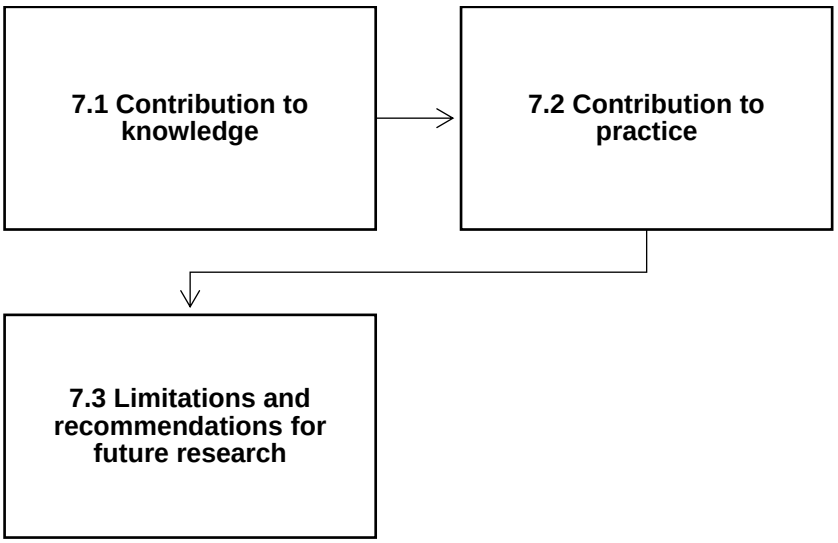


Figure 22: Conclusions chapter

Section 7.3 will point out limitations of the current study and recommend areas that might be interesting for future studies.

7.1 Contribution to knowledge

This thesis has investigated the trust of German companies in U.S. cloud providers from the perspective of buyers and sellers and contributes to the body of the literature that has called for studies of trust in business to business relationships (e.g. Geyskens, Steenkamp, and Kumar (1998), Wilson (1995), Seppänen et al. (2007)). The main goal of the current study was to determine the importance of the notion of trust for German buyers regarding the adoption of U.S. cloud services (RO1a). In this investigation, the aim was to assess the influence of the cultural differences between the U.S. and Germany (RO1b) and the impact of the sector of the German company (RO1c) on the trust of German buyers in U.S. cloud sellers. The second objective was to explore the trust relationship between German companies and U.S. cloud products (RO2a), U.S. cloud provider companies (RO2b), the local sales representatives of the U.S. cloud providers (RO2c) and the U.S. government (RO2d). Another purpose of the current study was to identify ways how U.S. cloud providers can improve the trust relationship with German companies (RO3) and develop a conceptual framework for buyer-seller trust in the context of international public cloud computing services (RO4). The findings from this study make the following contributions to the current literature.

Methodological

The first contribution is methodological. As reported in the literature review chapter, most of the inter-organisational and inter-personal research on trust is solely based on quantitative methods. As noted by Wright and Ehnert (2010, p. 119), “the dominant discourse among trust researchers is positivistic”. Furthermore, Möllering (2002, p. 158) concluded that “the role of trust is not easily quantifiable and therefore this area of research can be expected to benefit greatly from qualitative studies”. And, according to Seppänen et al. (2007, p. 261), since “the concept of trust is apparently not easily quantifiable, it seems obvious that qualitative empirical studies and piloting are also called for before quantitative surveys are carried out”. Therefore, the current study contributes to existing knowledge by applying qualitative methods to study the origins and reasons for trust or distrust between the parties involved. Since the qualitative research method is particularly suited to get a deep understanding of human behaviour and individual meaning in a real-world context, this method was particularly helpful to interpret the social and cultural process in the relationship between German

companies and U.S. cloud providers. The rationale for applying a qualitative study was to explore the roots and motives for trust or distrust between the parties involved. This approach led to research findings such as the importance of culture and sector which would not have been discovered in a purely quantitative research.

Another methodological contribution was the collection and analysis of dyadic data from buyers and sellers. As argued by Ashnai et al. (2016), due to the difficulty of collecting dyadic data, most current buyer-seller relationship studies are based on monadic data. The current research is following the recommendations by T. Gao et al. (2005) and Ashnai et al. (2016) to focus on the collection of dyadic data and include the perspectives of both the buyers and the sellers. From an academic perspective, this research is one of the few contributions to trust literature that comes from a qualitative angle to learn more about trust issues from the perspective, and the words, of German companies and U.S. sellers themselves. This approach allowed to analyse conflicting views and consensus between the IT managers of German companies and the local sales representatives of U.S. cloud providers regarding the adoption of U.S. public cloud services.

Furthermore, this is one of the very few empirical studies on buyer-seller trust carried out in non-English speaking countries. Since cross-cultural validation of constructs has sometimes led to controversial findings, this research will hopefully contribute to the body of knowledge in this field.

Trust in buyer-seller business to business relationships

The present study confirms previous findings (e.g. Ganesan (1994), E. Anderson and Weitz (1989), Sako (1998), A. Zaheer et al. (1998)) and contributes additional evidence that suggests that trust is a vital component in buyer-seller relationships and has significant impact on the buyer’s purchasing decision. More specifically, the current research contributes to existing knowledge by analysing buyer-seller trust in the context of public cloud computing services in an international setting. Both groups, the respondents of the buyers and the sellers, reported that trust was an imperative for IT services contracts in general but of even greater importance for cloud computing sales.

Moreover, these results agree with the findings of other studies, in which trust is described as essential for social relations and human interaction (e.g. Blau (1964), Golembiewski and McConkie (1975), Lewis and Weigert (1985b). The findings of the current research also confirmed the fragility of trust that was found in previous studies (e.g. Baier (1986), Lewicki and Bunker (1996), Dietz and Gillespie (2012)).

The importance of the concept of trust for German companies in U.S. cloud providers was directly influenced by the aspects of the cultural differences between the U.S. and Germany as well as the sector the German companies were operating in. This study contributes to the literature by showing the relevance of these two aspects of trust when explaining the behavioural characteristics of German buyers.

Culture and trust

The current findings add to a growing body of literature on the specifics of national culture and the impact on trust. Based on the cultural dimensions of Hofstede (2018), the current research analysed the perspective of the buyers and sellers on the impact of the cultural differences between Germany and the U.S. on trust and public cloud adoption. The present findings seem to be consistent with other research which found that the process of trust building and the levels of trust are influenced by national culture (e.g. Triandis (1972), Dyer and Chu (2000), Handfield and Bechtel (2002), S. Zaheer and Zaheer (2006), Dietz et al. (2010)). Furthermore, the current research supports earlier studies that portray cultural differences as obstacles or barriers to trust building (e.g. A. Bird and Osland (2005); Osland and Bird (2000)).

This is the first time that Hofstede's cultural dimensions have been used to explore the trust relationship between German companies and U.S. cloud providers. In terms of the **individualism** dimension, the present findings seem to be consistent with other research which found that the U.S. culture is highly individualistic and gives priority to personal goals (e.g. Triandis (2001), Hofstede (2018)). Consequently, as reported by the key informants of the current research, the reluctance to adapt their individualistic goals to the needs of foreign markets could have a negative impact on the adoption of U.S. cloud services by German companies. Moreover, these findings further support the idea of differentiation between in-group and out-group members as an aspect of the individualism dimension (e.g. Yamagishi and Yamagishi (1994), Inglehart et al. (1998), Dinev et al. (2006). This would imply that German companies, as members of

a more collectivistic culture, see U.S. cloud providers as foreign and out-group entities and develop less trust in those companies than in German providers or their own private data centres. Additionally, the findings of the current study are consistent with those of Krasnova et al. (2012) who found that the amount of information that U.S. citizens are willing to disclose is significantly higher than the data shared by German citizens. However, the findings of the current study do not support the previous research by e.g. Milberg et al. (2000) and Posey et al. (2010) who found that cultures with higher individuality scores are more concerned about data privacy than collectivistic cultures. The current research could not resolve this conflict but contribute to the number of studies that examine the role of the individualism-collectivism dimension regarding sharing personal information.

In terms of **uncertainty avoidance**, the current research seems to confirm previous studies on the relationship between uncertainty avoidance and risk taking (e.g. H. Park (1993), Hofstede (2003a)). According to buyers and sellers, Germans, as a culture with a high score of uncertainty avoidance, are described as risk-averse and cautious. This would support the idea of the “German Angst”, describing the pessimism, despondency and wariness in the German society (S. Bode, 2006; Fersch, 2012; Müller & Witmer-Goßner, 2015). Furthermore, the findings suggest that the strict privacy laws in Germany reflect the German culture and seem to confirm the association between German culture and the higher need for structure, formal rules and regulations (e.g. Bellman et al. (2004), Lim et al. (2004), Dinev et al. (2009), Krasnova and Veltri (2011)). Additionally, this study enhances our understanding of the interplay between culture and technology. The findings of the current research are consistent with those of other studies suggesting that cultures with a high level of uncertainty avoidance such as Germany would be less open to the adoption of new innovations and technologies (e.g. Hofstede (2003a), Leidner and Kayworth (2006), Cao and Everard (2008). The U.S., on the other hand, has a low score in the uncertainty avoidance dimension and was found to have a high openness for new ideas and innovative products. These cultural differences might partially explain the relatively low cloud adoption in Germany and why U.S. cloud services are considered superior to German cloud offerings.

The large deviation in the **long-term orientation** dimension might be another explanation for the preference of private data centres over public cloud services by German companies. The buyers explained that they made significant investments in their own IT infrastructure and would try to recreate the functionalities of public cloud services with their own equipment and staff. The present findings seem to be consistent with other research which found that cultures such as Germans with a high score on the long-term orientation dimension would be more focused on protecting their investments and take more time for adopting new technologies (Hofstede & Minkov, 2010). Hence, if the IT strategy of German companies is aiming for long-term solutions, a migration to the public cloud would require a systematic analysis of the benefits and risks, as well as a dedicated project, budget and timeline for the migration. Additionally, the findings of the current research corroborate the ideas of Hofstede (2018, p. 2), who suggested that many U.S. citizens have very strong opinions about "what is good and evil". The German buyers gave several examples where they experienced strong or conflicting views in the U.S. culture such as gun control law and public health care systems.

In terms of **indulgence**, the current study seems to confirm Hofstede (2018) who claimed that the German culture is restrained in nature and has a tendency to pessimism and cynicism. The seller respondents described their German customers as being negative, cautious, sceptical and conservative and claimed that German companies would believe that they could do things better themselves.

In addition to Hofstede's cultural dimensions, the current research identified two additional aspects that had an influence on the trust of German companies in U.S. cloud providers. The findings observed in this study mirror those of the previous studies that have examined the effect of the German **history** on the German culture (e.g. Krasnova and Veltri (2010), R. Anderson (2008), Lichter et al. (2016)). These results agree with the findings of other studies, in which the German culture, particularly in terms of data privacy matters, was strongly influenced by its history. According to the German buyers, U.S. citizens could not understand the position of German companies towards data privacy since they did not share the same history with the Nazi Secret State Police (GeStaPo) and the State Security of the GDR (StaSi) and did not experience national security agencies spying on their own citizens.

Therefore, these findings enhance our understanding of the effect of the global surveillance disclosures on the adoption of U.S. cloud services in the light of the German history.

Furthermore, the results of this study indicate that the **age** of a business decision maker has an influence on technology adoption in general and the trust in public cloud solutions in particular. These results agree with the findings of other studies, in which younger people were more open to new technologies and less concerned about negative consequences (e.g. Moscardelli and Divine (2007), Lenhart and Madden (2007a), Palfrey and Gasser (2011), Rodriguez and Obradovac (2017), Van den Broeck et al. (2015)). However, additional research is required to analyse the impact of the age of a buyer on the trust and privacy concerns he or she has with respect to public cloud services.

Taken together, the present study confirms previous findings and contributes additional evidence that suggests that the process of building and maintaining trust are influenced by national culture.

Sector and trust

This study contributes to the theory of business to business relationships by addressing the question of the influence of the sector on public cloud adoption in a cross-industry study. Despite its exploratory nature, this study offers some insight into the influence of the sector or industry of a German company on the adoption of U.S. cloud services. The present study confirms previous findings and contributes additional evidence that suggests that certain sectors are more reluctant with entrusting their data to U.S. cloud providers than others. The current research identified the financial services industry as particularly hesitant to adopting public cloud services. The influencing factors found in this study include legal constraints and the fear of economic espionage. These findings enhance our understanding of the impact of the sector of the buyer as a deciding factor for purchase decision making mechanisms in the cloud computing area and possibly other businesses.

The **size** of a company was mentioned as an additional factor influencing the decision regarding public cloud adoption. However, this relationship was only mentioned by a few participants and requires further research.

Among the contributions to the current literature discussed above, this work contributes to existing knowledge in the following four key areas. The current research not only distinguished between interpersonal and interorganizational trust as demanded by several researchers such as Doney and Cannon (1997), Ganesan and Hess (1997) and A. Zaheer et al. (1998), but also took the trust in the product or service into account. Moreover, this study expanded the trust relationships by a fourth dimension, the trust in the foreign government. This is the first time that these four relationships have been used to explore the trust of German buyers in U.S. cloud services.

Inter-organisational trust

This work contributes to existing knowledge of inter-organizational trust by providing the perspectives of buyers and sellers on the trust of German companies in U.S. cloud providers.

The present findings seem to be consistent with other research which found that the perceived **ethical behaviour** of a selling company played an important role in creating trust in the selling company (e.g. Lagace et al. (1991), Moorman et al. (1993), Kennedy et al. (2001)). Following the global surveillance disclosures, **U.S. cloud providers** had difficulties to ensure to German buyers that they did not cooperate with the U.S. intelligence agencies and that their ethical standards would not allow to give customer data to third parties. Additionally, these results agree with the findings of other studies, in which the **reputation** of a business partner has a strong positive impact on the level of trust (e.g. Aulakh et al. (1996), Maister et al. (2000), Kwon and Suh (2004)). However, since cloud computing is a relatively new service, potential buyers do not have much historical information that they can base their decisions on and, according to the respondents, U.S. cloud providers need to provide customer references and success stories to increase trust.

The global surveillance disclosures were identified as an exogenous source outside the scope of the buyer-seller relationship which caused **environmental uncertainty**. The findings observed in this study mirror those of the previous studies that have examined the negative effect of environmental uncertainty on the trust-performance relationship (e.g. Krishnan et al. (2006). The results of this study indicate that the environmental uncertainty regarding the potential access of U.S. government

agencies to data stored at U.S. cloud providers gave **German cloud providers** an exclusive selling proposition. These findings further support the idea that **emotional factors** (“gut feeling”) played a significant role in the decision making process of the German buyers and that the high score on the uncertainty avoidance scale by Hofstede (2018) and the “German Angst” (S. Bode, 2006) were exploited by German cloud providers. However, the findings of the current study do not support the stance that German cloud providers were the main profiteers of the surveillance scandal.

Another important finding was that despite the business benefits of public cloud services, the buyer respondents of the current research preferred to keep their data in their own data centre or **private cloud**. These results agree with the findings of market research studies, in which German companies made significant investments in their own private cloud infrastructure. Furthermore, the findings observed in the current research mirror those of previous studies that have examined the effect of **decision-making uncertainty** on purchase behaviours (e.g. T. Gao et al. (2005)). The results of this study indicate that German buyers were not willing to make any risky decisions such as moving their data to a U.S. cloud service since they did not trust the U.S. cloud providers. Another barrier to public cloud adoption that was identified in the current research was **investments costs**. This also accords with earlier observations, which showed that building supplier trust imposes costs on buyers and requires effort to find, evaluate, and select a new supplier (e.g. Dyer and Chu (2003), Handfield and Bechtel (2002)). These findings further support the idea that trust is positively related to flexibility and that buyer’s trust in the supplier may suffer with increased supplier dependence in form of the so called vendor lock-in with public cloud services (e.g. Young-Ybarra and Wiersema (1999); Dyer and Chu (2003); T. Gao et al. (2005).

Inter-personal trust

Previous research identified inter-personal trust as a key factor for the buyer’s purchase behaviour or even the most important variable of all trust relationships (e.g. Swan et al. (1985), Dwyer et al. (1987), Crosby et al. (1990), Ganesan and Hess (1997)). However, the findings of the current study do not support the previous research.

This study follows the methodological guidance in the literature to take the buyer’s perspective into consideration (Friend et al., 2018; Wood et al., 2008) and empirically

demonstrates that the buyers did not see the salespeople as helpful in their purchase decision-making process. The statements of the buyers interviewed in the current research suggest that the **local sales representatives** of the U.S. cloud providers did not add much value and could not improve the trust of the buyer in the selling company. Moreover, this study has been unable to demonstrate that building a **personal relationship** between salesperson and the buyer would be critical for building trust relationships between the parties as suggested by previous research (e.g. Newell et al. (2011), D.-J. Yang and Wu (2014)). Instead, the buyers stated that they would not get much benefit from the relationship with the cloud seller. This is, however, in contrast to the views of the seller respondents of the current research and the literature on personal relationships and information sharing (e.g. Coote et al. (2003), Kwon and Suh (2004)). Furthermore, the findings of the current study are consistent with those of Kennedy et al. (2001) who found that buyers who perceived themselves as knowledgeable about the product prior to its purchase had lower levels of trust of the salesperson. Several buyer respondents stated that they would **inform themselves** about a product or service without the need of a salesperson. This study concluded that public cloud services are particularly suited for buyers who prefer to inform themselves or purchase a product online without salesperson interaction. Besides, the results of the current research are consistent with those of other studies which that **selling orientation** has a negative impact on buyer trust in the salesperson (e.g. Guenzi and Georges (2010), Tam and Wong (2001), Kennedy et al. (2001)). The current research found that buyers opposed the idea of salespeople trying to convince them that public cloud services are secure and would solve their business problems. These results are in contrast to the majority of studies where salesperson trust is noted to be particularly critical for buyer-seller relationships.

In contrast to the findings above where the respondents of the German companies stated that they did not need local sales representatives of the U.S. providers, the buyers stated that the sellers should have **market and sector knowledge**. Therefore, these results agree with the findings of other studies, in which the **expertise** of a sales representative may help developing trust by creating confidence in the buyer that the salesperson is knowledgeable (e.g. Moorman et al. (1993), A. H. Liu and Leach (2001), Dowell et al. (2013)) and thereby reducing the buyer's feelings of uncertainty and vulnerability (e.g. Crosby et al. (1990), Swan et al. (1999)). These findings further

support the idea that buyer perceptions of supplier and salesperson expertise and trust are higher when the purchase is minimally important than when the purchase is extremely important (e.g. Belonax et al. (2007)). Since the adoption of public cloud services could be rated as an **important purchase decision**, the local sales representative of the U.S. cloud provider would be less relevant. The practical applications resulting from these findings in terms of **training**, **hiring** and **long-term commitment** will be presented in the section on the contribution to practice.

Product trust

The current research followed the recommendation of Plank et al. (1999) and not only studied inter-personal trust and inter-organisational trust, but also considered the expected functions and obligations associated with the offered products and services.

The first contribution to knowledge regarding product trust is that German companies acknowledged the technological and business benefits of public **cloud computing technology** and that they had trust in the cloud ecosystem as defined by Lansing and Sunyaev (2016). Additionally, the findings further support the idea that selling services and **intangible goods** such as public cloud services involves long-term commitment (e.g. Crosby et al. (1990), Chow and Holden (1997), Palmatier et al. (2006)). For example, the buyers reported that their in-house IT departments would understand their business better than any external providers.

The findings further agree with the findings of studies which found that the most advanced public cloud computing solutions are offered by **U.S. cloud providers**, e.g. European Commission (2015b)). An implication of this finding is that a lack of functionalities in U.S. cloud services or low **product quality** was probably not a reason why German companies would avoid U.S. cloud providers. However, the findings of the current study do not support the previous research on **brand trust** (e.g. Chaudhuri and Holbrook (2001), Delgado-Ballester and Luis Munuera-Alemán (2001)). Although the buyers argued that no German company could compete with the services of U.S. cloud providers, this view did not result in purchase loyalty or made them feel secure as reported in previous studies.

The present study confirms previous findings and contributes additional evidence that suggests that IT departments see **shadow IT** as a significant risk to IT security (e.g.

Shaikh (2018), Walterbusch et al. (2017), D. Oliver and Romm (2002), Strong and Volkoff (2004)). The fact that almost all buyers admitted that shadow IT cloud services were used in their companies suggests that there is a wish or need from the employees of the German companies to use cloud services that provide functionalities which they did not get from their own corporate IT departments. Taken together, these findings suggest that the quality and business benefits of U.S. cloud services are not the reason for the low adoption of public cloud services by German companies.

Foreign government trust

Perhaps the most significant contribution of the current research is related to the trust of German companies in the U.S. government. This study has demonstrated, possibly for the first time, that the trust between buyers and sellers can be levered out by the distrust in the foreign government. This finding is also a key component of the conceptual framework which shows that foreign government trust is the foundation for the other trust relationships.

The empirical findings in this study provide a new understanding of the impact of the **global surveillance disclosures** on the trust of German companies in U.S. cloud providers and the U.S. government. Both the buyers and the sellers reported that they were shocked by the intensity and extent of the NSA surveillance activities which led to a significant **mistrust**. The present findings seem to be consistent with other research which found that mistrust causes the buyer to take steps to protect his interests and takes time and effort on both sides, buyer and seller, to overcome (e.g. Swan et al. (1988), Abdul-Rahman (2005), Huerta-Canepa et al. (2011)). Moreover, the buyers argued that it would take many years to rebuild the trust they lost in U.S. companies and the U.S. government. These results agree with the findings of other studies, in which trust failures typically take years to resolve and are very costly (e.g. Dietz and Gillespie (2012)). Moreover, the present study provides additional evidence with respect to the impact of the global surveillance disclosures on **cloud adoption** in Germany. The buyers reported that Snowden revelations destroyed their trust in U.S. cloud services and that they stopped all cloud migration projects. The sellers confirmed that the cloud business in Germany slowed down because of the surveillance scandal. These results agree with the findings of other studies which

found that the already existing concerns about cloud technology had been reinforced after the incident (e.g. El-Gazzar (2016), PwC (2013b), KPMG (2014)).

One unanticipated finding was the special significance of the threat of **economic espionage** for German companies in connection with U.S. cloud services. Several respondents used the word “fear” to describe their thoughts and feelings about economic espionage and cited the risk of intellectual property theft as a major obstacle for cloud adoption. The present findings seem to be consistent with other research which found that German economy is particularly dependent on exports of high-tech products (Bryant, 2013c) and that the protection of intellectual property and patents are of constant concern for German companies (Bryant, 2013b; Destatis, 2017). Furthermore, the buyers stated that they would not save any business-critical information in the cloud. In accordance with the present results, previous studies have demonstrated that when companies face greater risk of knowledge appropriation by their business partners, they will engage in behaviours of **knowledge protection** (e.g. Norman (2002)). The findings also accord with the earlier observations on the role of the sector/industry, which showed that the manufacturing industry, the automotive sector and the automotive supplier industry were especially afraid of economic espionage. These findings further support the idea of the **value of data** with regard to the ongoing digitalisation of traditional businesses (e.g. Van der Aalst (2014), Nasheri and Blumstein (2005), Shackelford and Russell (2014), Davis et al. (2017)).

Both buyers and sellers agreed that they lost their trust in the **U.S. government** and that it was unlikely that the U.S. government would make any substantial changes to the surveillance law anytime soon. This finding corroborates the ideas of Kshetri (2013, p. 5), who suggested that “some governments are using the coercive power of the state to use the cloud in spying on citizens”. Furthermore, the respondents argued that the U.S. government would not change anything without the pressure of the U.S. technology sector. These findings further support the idea that, with exception of the EU, legislation around data privacy and cloud computing services is still a national domain and that international agreements are rare (Cheung & Weber, 2015; Jaeger et al., 2008; Millard, 2013). Recent developments in the U.S. politics after the election of President Donald Trump did not show any significant changes to the U.S.

surveillance laws or agreements with U.S. cloud providers (e.g. Heidrich (2017), Bager (2017), Ismail (2017)).

Another key finding regarding government trust was that the buyers and sellers were frustrated about the lack of action by **German and EU government** officials. From the point of view of the respondents of the current research, the words and actions of the German and EU politicians did not produce the desired results of protecting the German and EU citizens from surveillance activities and re-establishing trust in their government. Additionally, the respondents did not have confidence that the German government would have the necessary **technological knowledge** to increase the competitiveness of the German information technology sector. These results are consistent with those of other publications which suggest that politicians are increasingly uninformed about the technology and business models of cloud service providers and technology companies (Brühl, 2018; Cawley, 2018b; C. Lee, 2016; Pring-Mill, 2018). However, despite the criticisms related to the reactions of EU and German government officials, the European agreement on the General Data Protection Regulation (GDPR) might not have been possible without the Snowden revelations.

Conceptual framework

This study contributes to existing knowledge in trust in buyer-seller relationships by developing a conceptual framework that incorporates two different groups of characteristics (trust relationships and influential factors) that play a role enhancing business to business relationship outcomes. Furthermore, the framework could help selling companies to enhance their competitive advantage and achieve superior sales outcomes by creating and managing trust-based relationships with their customers.

The results suggested that of all four trust relationship types analysed, **foreign government trust** had the greatest impact on the buyer's purchasing decision and overruled the other three classic trust relationship types. The research findings suggested a hierarchy of importance of the trust relationships with foreign government trust being the most important, company trust being the second most important, the trust in the product/service being the third most important and salesperson trust being the least important trust relationship. The findings of the current study do not support previous research which found that salesperson trust was as important or even more

important than the other trust relationships. Furthermore, the framework illustrates that all four trust relationships are influenced by external factors such as the **cultural** background of the buyer and seller and the **sector** of the buying company. Another conclusion was that the most significant trust relationship, the trust in the foreign government, could only be **indirectly** influenced by the seller. While the seller has a **direct** influence on the recruitment and training of their salespeople, the features and quality of their products/services as well as the brand and public image of the company, there is no direct control of the policies and actions of the government bodies.

Altogether, despite its exploratory nature, this study offers some insight into the limitations of the traditional trust relationship models and enhance our understanding of the impact of third parties such as the foreign government on the trust relationship between buyers and sellers. Future research should therefore take the trust relationships to foreign government entities into account when studying business to business trust in an international context.

7.2 Contribution to practice

The findings of this study have a number of important implications for future practice. A key objectives of this research (RO3) was to contribute to practice by identifying ways how U.S. cloud providers can improve the trust relationship with German companies. The potential beneficiaries of this research study are mainly U.S. cloud providers. However, these findings might also have implications for other sectors or industries facing similar challenges.

Data centre location

The first important practical implication of the current research is a definite need for local cloud data centres in Germany. The availability of a domestic cloud data centre was one of the most frequently requested actions and most of the key informants wished for their data to be stored within German boarders. As discussed above, a German data centre gives the German companies a better feeling about the security of their data, even if there are no legal requirements for that. The cloud sellers stated that a domestic data centre has mainly psychological reasons and would help to provide the German decision makers with a better gut feeling. This information can be

used to develop targeted interventions aimed at the emotional components of the decision-making progress. According to the sellers, the impact of a German data centre would be even higher if it would be completely run by a German company with German personnel and only the hardware and software would be provided by a U.S. company.

To win the trust of their German customers, U.S. cloud providers should therefore either build their own data centre in Germany or partner with a local provider to offer U.S. cloud computing solutions for the German market. Another approach could be to join EU or German government initiatives to build a federated and open cloud data infrastructure with an ecosystem of local and foreign cloud providers. As discussed in the previous chapter, some U.S. cloud providers are already building local data centres in Germany or work together with local IT service providers to store company data in Germany. This development can be interpreted as a positive sign that U.S. cloud providers are listening to the demands of their German customer base.

Legal proceedings

Secondly, the interviewees expressed their concerns regarding the potential involvement of U.S. cloud providers in government surveillance activities. A reasonable approach to tackle this issue could be for the U.S. cloud providers to take legal proceedings against the U.S. government. As discussed in the previous chapter, the key informants in this study would welcome any initiatives of the U.S. cloud providers against any dubious U.S. law enforcement operations that involved European citizen data. A favoured approach expressed by the interviewees would be to take legal actions against any unlawful practices of the U.S. intelligence agencies and enforce transparency in ongoing investigations. The cloud sellers were also in favour of the proposed courses of action against the U.S. government.

As discussed earlier, a few U.S. cloud providers have already successfully refused to hand over data from European customers who had their data stored in a European data centre. Consequently, U.S. cloud providers should continue to collectively or individually challenge the global data collection reach of the U.S. government and protect the legal rights of their international customers. A key policy priority for U.S. cloud providers should therefore be to plan for the long-term care of their EU customer

base by creating an environment that protects the businesses of their customers from external forces.

Cloud computing contracts

There are a few critical changes which need to be made on the contractual level. As detailed in the previous chapter, contracts with U.S. cloud providers are often only available in English and are based on the law of foreign countries such as the U.S. or Ireland. This can be a criterion for excluding U.S. cloud providers in the vendor selection process of German companies. Several respondents clearly stated that they would demand their contracts with U.S. cloud providers to be written in German language and based on German law. However, while the German IT managers demanded the jurisdiction to be in Germany, the U.S. providers shied the risks and costs involved in applying German law.

It is, however, recommended for U.S. cloud providers, in order to win the trust of potential German customers, to offer contractual agreements with their German customers in German language and with German jurisdiction. This finding will probably also apply to other sectors or industries planning to make business with German or other European companies.

Data encryption

Another important practical implication is that customer data stored in the data centres of the U.S. cloud providers should not be accessible by the cloud provider but only by the cloud consumer. A great demand expressed by several interviewees was that the U.S. cloud providers should offer strong encryption technologies for their cloud services and encrypt all data at rest and in transit. The cloud consumers would like to be able to bring their own encryption keys and keep the keys within the walls of their companies. Strong data encryption could also solve some regulatory issues that certain sectors in Germany are facing. Recent cases of U.S. government officials asking U.S. technology companies for building backdoors into their software support this requirement.

While the cloud sellers supported the idea of data encryption in the cloud in general, they warned of the risks in losing the encryption keys, high administrative costs and a limited scope of functions when encrypting cloud data. Especially Software-as-a-

Service cloud solutions would have difficulties to index and edit data when it is encrypted with an external key. However, since data encryption promises to solve several data privacy issues, U.S. cloud providers should invest in developing data encryption technologies which combine cloud computing features with high security. In the future, fully homomorphic encryption systems could allow computations to be performed on encrypted data without the need to first decrypt the data.

Local sales representatives

Another managerial implication of the findings applies to the local salespeople of the U.S. cloud providers. The key set of findings, that the relationship between the buyer's propensity to trust and trust in the salesperson depends on the level of expertise and ethical behaviour of the salesperson, have implications for how sales managers should hire, train and manage salespeople.

The results of the current research agree with the findings of other studies, in which companies should design training concepts to help their salespeople building trust with their customers and become more competent and professional. Therefore, from a managerial perspective, the current research suggests that it is central to provide the right kind of training for salespeople, so they have the skill set and knowledge to engage with the buyer in the appropriate level of adaptive selling depending on the product, service and industry. While training is helpful, sales managers also need to be aware that their effectiveness is limited unless the right people are hired for the job. Given that not all salesperson skills can be trained, sales managers must focus on recruiting salespeople with the appropriate qualities. In accordance with the present results, previous studies have demonstrated that sales managers should also give salespeople sufficient time to build a personal long-term relationship with the buyer. The German companies had made negative experiences with the commitment and empowerment level of the local sales representatives of the U.S. cloud providers. A reasonable approach to tackle this issue could be to give local sales representatives more time to develop a personal relationship with their customers and by transferring greater decision-making power them.

Implications

As discussed earlier, artificial intelligence is probably emerging to the most important technology of the next decades. With cloud computing becoming increasingly powerful and ubiquitous, artificial intelligence will no longer operate in narrow use cases but connect various disciplines and rapidly acquire new capabilities. The data fuelling the artificial intelligence engine will most likely become the 21st century's most important resource. Since the development of better artificial intelligence models require more and more data, this bears the risk that those with access to the most and best data, large countries and companies, will gain a significant competitive advantage.

The German and other EU governments have called for "digital sovereignty" to U.S. technology companies to gain back control over their data and be less dependent on foreign companies and countries. They argue that, to protect national and economic interests, countries in the EU must be capable of individually safeguarding the security of its digital assets. However, the expanding number of information technologies developed outside of the EU and the increasing international data flows make it ever more difficult to implement any concepts of national sovereignty in the cloud computing and artificial intelligence space. Several years after the Snowden revelations many problems regarding data privacy and government surveillance reach remain unsolved and there is no sustained improvement in sight. In order to be competitive, German companies will need to either find ways to be less dependent on foreign technology companies or find ways to securely process their data at international technology providers that they can trust.

As discussed in the previous chapter, all four key actions recommended by the buyers are aiming to improve or obviate the need for the trust in the foreign government. However, since cloud technologies and corresponding legal requirements are constantly changing, U.S. cloud providers will need to implement further measures to convince German companies to store and process their data in U.S. cloud services. To win and maintain the trust of German companies, U.S. cloud providers will have to continuously identify ways to protect their data from third party access in a way that makes long-term investments in their cloud services appealing. A key policy priority might therefore be to involve the decision makers of potential cloud customers in the planning of future cloud services to win their trust.

7.3 Limitations and recommendations for future research

A few limitations need to be considered regarding the scope and design of the current research. Several paths for future research such as a wider group of respondents, the importance of salesperson interaction, and the perceived threat of economic espionage in other countries have already been suggested in the previous chapters.

The single point in time perspective of the current research inhibits the understanding of the trust formation process over a longer period of time. Therefore, a **longitudinal study** could offer the opportunity to learn about the different stages and dependencies in the trust formation process. As discussed in the previous chapter, cloud computing technologies and national legislations are subject to constant change and development. As such, future efforts to investigate the role of trust in a longitudinal fashion should look at moderating factors influencing the trust relationships.

Furthermore, the current study has only examined the trust of German companies in U.S. cloud providers and the study collected data from companies solely within Germany. Future research should therefore concentrate on the investigation of the trust relationships between U.S. cloud providers with **other countries** in the EU or countries outside the EU to determine if the theory holds true. Additionally, further research might explore the trust of German companies in cloud providers that are not registered in the U.S. but are based in another country inside or outside of the EU.

Another limitation of this study is that the numbers of respondents for each **sector** or industry were relatively small. The key informants of the current study came from various sectors such as banking, manufacturing and logistics but most sectors were only represented by a single interviewee. As discussed above, previous studies came to different results regarding the cloud adoption rate of specific sectors. Future research should therefore concentrate on the investigation of the influence of the sector on the trust in public cloud services with a larger number of respondents.

Additionally, this research investigated the different trust relationships between buyers and sellers in the context of public cloud computing services. The individual importance of the trust relationships discussed in the current research might differ with other **products/services** such as financial services or raw materials. Consequently, further research is needed to determine if the framework developed in this study fits with other products/services beyond cloud computing.

8 References

Abbadi, I. M., & Alawneh, M. (2012). A framework for establishing trust in the cloud. *Computers & Electrical Engineering, 38*(5), 1073-1087.

Abdul-Rahman, A. (2005). *A framework for decentralised trust reasoning.* University of London.

Ackerman, S., & MacAskill, E. (2016, November 11). Privacy experts fear Donald Trump running global surveillance network. Retrieved from https://www.theguardian.com/world/2016/nov/11/trump-surveillance-network-nsa-privacy

Acquisti, A. (2004). *Privacy in electronic commerce and the economics of immediate gratification.* Paper presented at the Proceedings of the 5th ACM conference on Electronic commerce.

Adjei, J. K. (2015). Explaining the role of trust in cloud computing services. *info, 17*(1), 54-67.

Agrawal, S., Agrawal, S., & Prabhakaran, M. (2015). *Cryptographic agents: Towards a unified theory of computing on encrypted data.* Paper presented at the Annual International Conference on the Theory and Applications of Cryptographic Techniques.

Aldrich, H. (2008). *Organizations and environments*: Stanford University Press.

Allik, J., & Realo, A. (2004). Individualism-collectivism and social capital. *Journal of cross-cultural psychology, 35*(1), 29-49.

Almanea, M. I. M. (2015). *The role of transparency and trust in the selection of cloud service providers.* (Ph.D.), Newcastle University.

Alvesson, M., & Sköldberg, K. (2009). *Reflexive Methodology: New Vistas for Qualitative Research*: SAGE Publications.

Amazon. (2014, October 23). Now Open – AWS Germany (Frankfurt) Region – EC2, DynamoDB, S3, and Much More. Retrieved from https://aws.amazon.com/blogs/aws/aws-region-germany/

Amazon. (2016, August 11). New – Bring Your Own Keys with AWS Key Management Service. Retrieved from https://aws.amazon.com/blogs/aws/new-bring-your-own-keys-with-aws-key-management-service/

Amazon. (2017a). AWS Blog. Retrieved from https://aws.amazon.com/blogs/aws/

Amazon. (2017b, May 5). SAP and Amazon Web Services. Retrieved from https://aws.amazon.com/sap/

Amazon. (2018, Mar 26). All AWS Services GDPR ready. Retrieved from https://aws.amazon.com/blogs/security/all-aws-services-gdpr-ready/

Anderson, E., Lodish, L. M., & Weitz, B. A. (1987). Resource allocation behavior in conventional channels. *Journal of marketing research*, 85-97.

Anderson, E., & Weitz, B. (1989). Determinants of continuity in conventional industrial channel dyads. *Marketing Science (1986-1998), 8*(4), 310.

Anderson, J. C., & Narus, J. A. (1990). A model of distributor firm and manufacturer firm working partnerships. *Journal of Marketing, 54*(1), 42.

Anderson, R. (2008). Terror, Justice and Freedom *Security Engineering: A Guide to Building Dependable Distributed Systems* (pp. 769-814): Wiley.

Andrikopoulos, V., Binz, T., Leymann, F., & Strauch, S. (2013). How to adapt applications for the Cloud environment. *Computing, 95*(6), 493-535. doi:10.1007/s00607-012-0248-2

Antonopoulos, N., & Gillam, L. (2017). *Cloud Computing: Principles, Systems and Applications*: Springer International Publishing.

AP. (2013, July 3). German minister: Drop US sites if you fear spying. *Associated Press*. Retrieved from http://bigstory.ap.org/article/german-minister-drop-google-if-you-fear-us-spying

APA. (2013). *Publication Manual of the American Psychological Association, Sixth Edition* (6th edition ed.): American Psychological Association.

Appelbaum, J., Blome, N., Gude, H., Neukirch, R., Pfister, R., Poitras, L., . . . Stark, H. (2013, October 27). Embassy Espionage: The NSA's Secret Spy Hub in Berlin. *SPIEGEL*. Retrieved from http://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205-3.html

Appelbaum, J., Poitras, L., Rosenbach, M., Stöcker, C., Schindler, J., & Stark, H. (2013, December 29). Inside TAO: Documents Reveal Top NSA Hacking Unit. *SPIEGEL*. Retrieved from http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html

Appelbaum, J., Stark, H., & Rosenbach, M. (2013, October 23). Berlin Complains: Did US Tap Chancellor Merkel's Mobile Phone? *SPIEGEL*. Retrieved from http://www.spiegel.de/international/world/merkel-calls-obama-over-suspicions-us-tapped-her-mobile-phone-a-929642.html

Apple. (2016, February 16). A Message to Our Customers. Retrieved from http://www.apple.com/customer-letter/

Ariño, A., De la Torre, J., & Ring, P. S. (2001). Relational quality: managing trust in corporate alliances. *California management review, 44*(1), 109-131.

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., . . . Stoica, I. (2010). Above the Clouds: A Berkeley View of Cloud Computing. *Communications of the ACM, 53*(4), 50-58.

Arnott, D. C. (2007). Research on trust: a bibliography and brief bibliometric analysis of the special issue submissions. *European Journal of Marketing, 41*(9/10), 1203-1240. doi:10.1108/03090560710773408

Arora, P., Biyani, R., & Dave, S. (2011). *To the Cloud: Cloud Powering an Enterprise*: McGraw-Hill Education.

Arthur, C. (2010, June 21). Cloud computing: time to stop sitting on your data. *The Guardian*. Retrieved from http://www.guardian.co.uk/cloud-computing/time-to-stop-sitting-on-your-data

Ashnai, B., Henneberg, S. C., Naudé, P., & Francescucci, A. (2016). Inter-personal and inter-organizational trust in business relationships: An attitude–behavior–outcome model. *Industrial Marketing Management, 52*, 128-139. doi:10.1016/j.indmarman.2015.05.020

Audi, R., Loughran, T., & McDonald, B. (2016). Trust, but verify: MD&A language and the role of trust in corporate culture. *Journal of Business Ethics, 139*(3), 551-561.

Auerbach, C., & Silverstein, L. B. (2003). *Qualitative Data: An Introduction to Coding and Analysis*: NYU Press.

Aulakh, P. S., Kotabe, M., & Sahay, A. (1996). Trust and Performance in Cross-Border Marketing Partnerships: A Behavioral Approach. *Journal of international Business studies, 27*(5), 1005-1032. doi:10.2307/155579

Avram, M.-G. (2014). Advantages and challenges of adopting cloud computing from an enterprise perspective. *Procedia Technology, 12*, 529-534.

Babbie, E. R. (1998). *The Practice of Social Research*: Wadsworth Publishing Company.

Bachmann, R., & Zaheer, A. (2006). *Handbook of Trust Research*: Edward Elgar.

Bager, J. (2017, April 13). Hinter die Mauern: Warum Sie im Jahr 2017 Ihre Daten in der EU behalten sollten [Behind the walls: Why you should keep your data in the EU in 2017]. Retrieved from https://www.heise.de/ct/ausgabe/2017-9-Warum-Sie-im-Jahr-2017-Ihre-Daten-in-der-EU-behalten-sollten-3678254.html

Baier, A. (1986). Trust and Antitrust. *Ethics, 96*(2), 231-260. doi:10.2307/2381376

Baker, J. (2011, December 2). European Distrust of US Data Security Creates Market for Local Cloud Service. Retrieved from http://www.pcworld.com/article/245335/european_distrust_of_us_data_security_creates_market_for_local_cloud_service.html

Baker, S. E., & Edwards, R. (2012). How many qualitative interviews is enough. *National Centre for Research Methods, (Unpublished)*.

Ball, J. (2013, October 25). NSA monitored calls of 35 world leaders after US official handed over contacts. *The Guardian*. Retrieved from http://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls

Ball, J. (2014, January 16). NSA collects millions of text messages daily in 'untargeted' global sweep. *The Guardian*. Retrieved from http://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep

Ball, J., Borger, J., & Greenwald, G. (2013, September 6). Revealed: how US and UK spy agencies defeat internet privacy and security. Retrieved from https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

Ball, J., Harding, L., & Garside, J. (2013, August 2). BT and Vodafone among telecoms companies passing details to GCHQ. *The Guardian*. Retrieved from http://www.theguardian.com/business/2013/aug/02/telecoms-bt-vodafone-cables-gchq

Bansal, G., & Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems, 49*(2), 138-150.

Barber, B. (1983). *The logic and limits of trust*: Rutgers University Press.

Barbour, R. (2013). *Introducing Qualitative Research: A Student's Guide*: SAGE Publications.

Barney, J. B., & Hansen, M. H. (1994). Trustworthiness as a Source of Competitive Advantage. *Strategic Management Journal, 15*, 175-190. doi:10.2307/2486817

Baskerville, R. F. (2003). Hofstede never studied culture. *Accounting, Organizations and Society, 28*(1), 1-14.

Batchelor, C. (2012, May 22). Privacy: US and EU clash on confidentiality. *The Financial Times.* Retrieved from http://www.ft.com/intl/cms/s/0/7887ea14-92c2-11e1-b6e2-00144feab49a.html#axzz2WxXC1sdZ

Bateman, C., & Valentine, S. (2015). The impact of salesperson customer orientation on the evaluation of a salesperson's ethical treatment, trust in the salesperson, and intentions to purchase. *Journal of Personal Selling & Sales Management, 35*(2), 125-142. doi:10.1080/08853134.2015.1010538

BBC. (2014a, July 4). Germany arrests man suspected of spying for US. Retrieved from http://www.bbc.com/news/world-europe-28160767

BBC. (2014b, January 26). NSA 'engaged in industrial espionage' - Snowden. Retrieved from http://www.bbc.com/news/25907502

BDO. (2014). *Cloud Computing – Digitalisierung im Mittelstand [Cloud Computing - digitization in SMEs]*. Retrieved from http://www.bdo.de/publikationen/cloud-computing-digitalisierung-im-mittelstand/

Beall, A. E. (2010). *Strategic Market Research: A Guide to Conducting Research That Drives Businesses*: iUniverse.com.

Behrens, S. (2009). Shadow systems: The good, the bad and the ugly. *Communications of the ACM, 52*(2), 124-129.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: a review of information privacy research in information systems. *Mis Quarterly, 35*(4), 1017-1042.

Bélanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. *The Journal of Strategic Information Systems, 11*(3-4), 245-270.

Beldad, A., de Jong, M., & Steehouder, M. (2010). How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust. *Computers in Human Behavior, 26*(5), 857-869.

Bell, J. (2005). *Doing your research project: a guide for first-time researchers in education, health and social science*: Open University Press.

Bellman, S., Johnson, E. J., Kobrin, S. J., & Lohse, G. L. (2004). International differences in information privacy concerns: A global survey of consumers. *The Information Society, 20*(5), 313-324.

Belonax, J. J., Newell, S. J., & Plank, R. E. (2007). The Role of Purchase Importance on Buyer Perceptions of the Trust and Expertise Components of Supplier and Salesperson Credibility in Business-to-Business Relationships. *The Journal of Personal Selling and Sales Management, 27*(3), 247-258.

Berg, C. (2018). Privacy and Speech *The Classical Liberal Case for Privacy in a World of Surveillance and Technological Change* (pp. 167-179): Springer.

Bergh, D. D., & Lawless, M. W. (1998). Portfolio restructuring and limits to hierarchical governance: The effects of environmental uncertainty and diversification strategy. *Organization Science, 9*(1), 87-102.

Berniker, M. (2018, Oct 16). Trump's China Tariff Wrath Presents Big Risk for US Tech Companies. Retrieved from https://www.forbes.com/sites/markberniker/2018/10/16/trumps-china-tariff-wrath-presents-big-risk-for-us-tech-companies/#67b481462350

Beugelsdijk, S., Koen, C., & Noorderhaven, N. (2009). A dyadic approach to the impact of differences in organizational culture on relationship performance. *Industrial Marketing Management, 38*(3), 312-323.

BfDI. (2010). Prüfung der Selbst-Zertifizierung des Datenimporteurs nach dem Safe Harbor-Abkommen durch das Daten exportierende Unternehmen [Examination of the data importer's self-certification according to the Safe-Harbor-Agreement by the company exporting data]. Retrieved from http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/290410_SafeHarbor.pdf

BfDI. (2011). *Orientierungshilfe Cloud Computing der Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder [Guidance Cloud Computing of the working groups and the media technology of the Conference of Data Protection Commissioners of the Federation and the States]* Retrieved from http://www.bfdi.bund.de/DE/Themen/TechnologischerDatenschutz/TechnologischeOrientierungshilfen/Artikel/OHCloudComputing.pdf

BfDI. (2013, July 24). Conference of data protection commissioners says that intelligence services constitute a massive threat to data traffic between Germany and countries outside Europe. Retrieved from http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/ErgaenzendeDokumente/PMDSK_SafeHarbor_Eng.pdf

BfV. (2017). *Brief summary 2016 Report on the Protection of the Constitution*: Federal Ministry of the Interior.

Bhosle, P. I., & Kasurkar, S. A. (2013). Trust in Cloud Computing. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 2*(4), pp: 1541-1548.

Bhowmik, S. (2017). *Cloud Computing*: Cambridge University Press.

Bialaszewski, D., & Giallourakis, M. (1985). Perceived communication skills and resultant trust perceptions within the channel of distribution. *Academy of Marketing Science. Journal (pre-1986), 13*(1), 206.

Bijlsma, K. M., & Van De Bunt, G. G. (2003). Antecedents of trust in managers: a "bottom up" approach. *Personnel Review, 32*(5), 638-664.

Billings, J. T. (2012). European protectionism in cloud computing: Addressing concerns over the PATRIOT ACT. *CommLaw Conspectus, 21*, 211-211.

Bird, A., & Osland, J. S. (2005). Making sense of intercultural collaboration. *International Studies of Management & Organization, 35*(4), 115-132.

Bird, C. M. (2005). How I stopped dreading and learned to love transcription. *Qualitative inquiry, 11*(2), 226-248.

Birnbaum, M. (2013, November 18). In Germany, legacy of Stasi puts different perspective on NSA spying. Retrieved from https://www.washingtonpost.com/world/in-germany-legacy-of-stasi-puts-different-perspective-on-nsa-spying/2013/11/18/a0b1b37c-4940-11e3-b87a-e66bd9ff3537_story.html

Blackmer, W. S. (2016, May 5). GDPR: Getting Ready for the New EU General Data Protection Regulation. Retrieved from https://www.infolawgroup.com/2016/05/articles/gdpr/gdpr-getting-ready-for-the-new-eu-general-data-protection-regulation/

Blank, G., Bolsover, G., & Dubois, E. (2014). A new privacy paradox: Young people and privacy on social network sites.

Blau, P. M. (1964). *Exchange and Power in Social Life*: John Wiley & Sons.

Blois, K. J. (1999). Trust in business to business relationships: An evaluation of its status. *Journal of Management Studies, 36*(2), 197-215.

Blomqvist, K. (1997). The many faces of trust. *Scandinavian Journal of Management, 13*(3), 271-286. doi:10.1016/S0956-5221(97)84644-1

Blomqvist, K. (2002). *Partnering in the dynamic environment: The role of trust in asymmetric technology partnership formation.* (Doctor of Science), Lappeenranta University of Technology, Lappeenranta, Finland.

Bluhm, L. H. (1987). Trust, Terrorism, and Technology. *Journal of Business Ethics, 6*(5), 333-341. doi:10.2307/25071669

BMBF. (2015). Industrie 4.0. Retrieved from https://www.bmbf.de/pub/Industrie_4.0.pdf

Bode, K. (2013, October 25). Spioniert die NSA für Amerikas Konzerne? [Does the NSA spy on American corporations?]. Retrieved from http://www.zeit.de/wirtschaft/2013-10/nsa-wirtschaftsspionage

Bode, S. (2006). *Die deutsche Krankheit - German Angst [The German disease - German Angst]*: Klett-Cotta.

Böhm, M., Leimeister, S., Riedl, C., & Krcmar, H. (2011). Cloud Computing–Outsourcing 2.0 or a new Business Model for IT Provisioning? *Application Management*, 31-56.

Bok, S. (1979). *Lying: Moral Choice in Public and Private Life*: Vintage Books.

Böken, A. (2011). Patriot Act und Cloud Computing -- Zugriff auf Zuruf? [Patriot Act and cloud computing - access on demand?]. *iX, 01/2012*, 110. Retrieved from http://www.heise.de/ix/artikel/Zugriff-auf-Zuruf-1394430.html

Bond, M. H. (2001). Surveying the foundations: Approaches to measuring group, organizational, and national variation. In U. K. Miriam Erez, Henk Thierry (Ed.), *Work Motivation in the Context of A Globalizing Economy*. Psychology Press, 2012.

Boorom, M. L., Goolsby, J. R., & Ramsey, R. P. (1998). Relational communication traitsand their effect on adaptiveness and sales performance. *Journal of the Academy of Marketing Science, 26*(1), 16-30.

Borges, G. (2014). Cloud Computing und Datenschutz [Cloud computing and data protection]. *Datenschutz und Datensicherheit - DuD, 38*(3), 165-169. doi:10.1007/s11623-014-0069-x

Boss, R. W. (1978). Trust and managerial problem solving revisited. *Group & Organization Management, 3*(3), 331-342.

Bottom, W. P., Gibson, K., Daniels, S. E., & Murnighan, J. K. (2002). When talk is not cheap: Substantive penance and expressions of intent in rebuilding cooperation. *Organization Science, 13*(5), 497-513.

Boulton, C. (2016, September 2). U.S. cloud vendors adjust to Snowden effect, Privacy Shield. Retrieved from http://www.cio.com/article/3115756/cloud-computing/u-s-cloud-vendors-adjust-to-snowden-effect-privacy-shield.html

Bowers, S. L. (2006). Privacy and Library Records. *The Journal of Academic Librarianship, 32*(4), 377-383. doi:10.1016/j.acalib.2006.03.005

Bowler, S., & Karp, J. A. (2004). Politicians, scandals, and trust in government. *Political Behavior, 26*(3), 271-287.

Boyacigiller, N. A., Kleinberg, J., Phillips, M. E., & Sackmann, S. A. (2004). Conceptualizing culture: Elucidating the streams of research in international cross-cultural management. *Handbook for international management research, 2*, 99-167.

Boyatzis, R. E. (1998). *Transforming Qualitative Information: Thematic Analysis and Code Development*: SAGE Publications.

Bradach, J. L., & Eccles, R. G. (1989). Price, Authority, and Trust: From Ideal Types to Plural Forms. *Annual Review of Sociology, 15*, 97-118. doi:10.2307/2083220

Bradshaw, S., Millard, C., & Walden, I. (2011). Contracts for clouds: Comparison and analysis of the terms and conditions of cloud computing services. *International Journal of Law and Information Technology, 19*(3), 187-223.

Branscombe, M. (2015, September 28). Is BYOK the key to secure cloud computing? Retrieved from http://www.cio.com/article/2986308/cloud-security/is-byok-the-key-to-secure-cloud-computing.html

Branzei, O., Vertinsky, I., & Camp II, R. D. (2007). Culture-contingent signs of trust in emergent relationships. *Organizational behavior and human decision processes, 104*(1), 61-82.

Brauck, M., Deckstein, D., Dohmen, F., Nezik, A.-K., Rosenbach, M., Schiessl, M., & Schmitt, J. (2013). Der Feind in meinem Netz [The enemy in my network]. *DER SPIEGEL, 32*.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative research in psychology, 3*(2), 77-101.

Braynov, S., & Sandholm, T. (2002). Contracting with uncertain level of trust. *Computational Intelligence, 18*(4), 501-514.

Breland, A. (2017, Jan 8). Senate bill would ease law enforcement access to overseas data. Retrieved from http://thehill.com/policy/technology/344823-senators-introduce-new-bill-to-force-law-enforcement-to-obtain-americans

Brickau, R., Huth, S., Tysiak, W., & Chaston, I. (2003). The three Dimensions of Trust in Buyer-seller Relationships in a Service Environment — Preliminary Findings of an Empirical Investigation. In U. Kamenz (Ed.), *Applied Marketing: Anwendungsorientierte Marketingwissenschaft der deutschen Fachhochschulen* (pp. 173-186). Berlin, Heidelberg: Springer Berlin Heidelberg.

Brühl, J. (2018, Jan 5). Die deutsche Politik braucht ein Sicherheitsupdate. Retrieved from https://www.sueddeutsche.de/digital/leak-daten-hacker-politik-1.4276010

Bryant, C. (2013a, July 28). European data protection under a cloud. *The Financial Times*. Retrieved from http://www.ft.com/cms/s/0/dbee868a-f43c-11e2-8459-00144feabdc0.html#axzz2z7XOXPUy

Bryant, C. (2013b, August 5). Germans' fear of American spying surges. *The Financial Times*. Retrieved from http://www.ft.com/intl/cms/s/0/d1a163ac-fdea-11e2-a5b1-00144feabdc0.html#axzz2z7XOXPUy

Bryant, C. (2013c, November 1). NSA claims put German business on guard. *The Financial Times*.

Bryant, C. (2013d, October 31). NSA revelations boost corporate paranoia about state surveillance. *The Financial Times*. Retrieved from http://www.ft.com/intl/cms/s/0/ec02a8ca-422b-11e3-bb85-00144feabdc0.html#axzz30ZCwgAaq

Bryman, A., & Bell, E. (2007). *Business research methods*: Oxford University Press.

Bryman, A., & Bell, E. (2011). *Business Research Methods 3e*: OUP Oxford.

BSI. (2013). Cloud Computing Grundlagen [Cloud Computing Basics]. *Bundesamt für Sicherheit in der Informationstechnik.* Retrieved from https://www.bsi.bund.de/DE/Themen/CloudComputing/Grundlagen/Grundlagen_node.html

Buchko, A. A. (1994). Conceptualization and measurement of environmental uncertainty: An assessment of the Miles and Snow perceived environmental uncertainty scale. *Academy of Management Journal, 37*(2), 410-425.

Bundesregierung. (2013, June 13). Pressekonferenz von Bundeskanzlerin Merkel und US-Präsident Obama [Press conference of Chancellor Merkel and US President Obama]. Retrieved from https://www.bundesregierung.de/ContentArchiv/DE/Archiv17/Mitschrift/Pressekonferenzen/2013/06/2013-06-19-pk-merkel-obama.html

Bundesregierung. (2014, January 29). Regierungserklärung von Bundeskanzlerin Merkel [Declaration of the Federal Chancellor Merkel]. Retrieved from https://www.bundesregierung.de/Content/DE/Regierungserklaerung/2014/2014-01-29-bt-merkel.html

Burton, D. (2000). The use of case studies in social science research. In D. Burton (Ed.), *Research Training for Social Scientists: A Handbook for Postgraduate Researchers*: SAGE Publications.

Busch, P., & Wilson, D. T. (1976). An Experimental Analysis of a Salesman's Expert and Referent Bases of Social Power in the Buyer-Seller Dyad. *Journal of marketing research, 13*(1), 3-11. doi:10.2307/3150896

Bush, G. W. (2001). Statement by the President in His Address to the Nation [Press release]. Retrieved from http://georgewbush-whitehouse.archives.gov/news/releases/2001/09/20010911-16.html

Bush, G. W. (2007, July 28). President's Radio Address. *The White House.* Retrieved from http://georgewbush-whitehouse.archives.gov/news/releases/2007/07/20070728.html

Business-Cloud. (2011, July 18). Datenweitergabe an die USA: Angst vor Online-Sheriff [Data transfer to the US: fear of online sheriff]. *Business-Cloud.de.* Retrieved from http://www.business-cloud.de/datenweitergabe-an-die-usa-angst-vor-online-sheriff/

Büst, R. (2015, November 11). Microsoft zeigt Amazon, Salesforce und Co. wie es richtig geht [Microsoft shows Amazon, Salesforce and others how to do it right]. Retrieved from http://www.computerwoche.de/a/microsoft-zeigt-amazon-salesforce-und-co-wie-es-richtig-geht,3218970

Büst, R. (2016, April 12). Public Cloud-Anbieter im deutschen Mittelstand [Public cloud providers for the German SMEs]. Retrieved from http://www.computerwoche.de/a/public-cloud-anbieter-im-deutschen-mittelstand,3226485

Butler, J. K., Jr. (1991). Toward Understanding and Measuring Conditions of Trust: Evolution of a Conditions of Trust Inventory. *Journal of Management, 17*(3), 643.

Cadwalladr, C., & Graham-Harrison, E. (2018, Mar 17). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. Retrieved from https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Caldwell, C., & Clapham, S. E. (2003). Organizational trustworthiness: An international perspective. *Journal of Business Ethics, 47*(4), 349-364.

Cannon, J. P., & Perreault Jr, W. D. (1999). Buyer-seller relationships in business markets. *Journal of marketing research*, 439-460.

Cao, J., & Everard, A. (2008). User attitude towards instant messaging: The effect of espoused national cultural values on awareness and privacy. *Journal of Global Information Technology Management, 11*(2), 30-57.

Carroll, R. (2013, August 31). Microsoft and Google to sue over US surveillance requests. Retrieved from https://www.theguardian.com/law/2013/aug/31/microsoft-google-sue-us-fisa

Carson, D. (2001). *Qualitative marketing research*: SAGE.

Cassell, C., & Symon, G. (2004). *Essential guide to qualitative methods in organizational research*: Sage.

Castro, D. (2013). How Much Will PRISM Cost the U.S. Cloud Computing Industry? *The Information Technology & Innovation Foundation (ITIF).* Retrieved from http://www2.itif.org/2013-cloud-computing-costs.pdf

Cate, F. (1994). The EU Data Protection Directive, Information Privacy, and the Public Interest. *Iowa L. Rev., 80*, 431.

Caverlee, J., & Webb, S. (2008). *A Large-Scale Study of MySpace: Observations and Implications for Online Social Networks.* Paper presented at the ICWSM.

Cawley, C. (2018a, Dec 11). The Best (and Worst) Questions Congress Asked Google. Retrieved from https://tech.co/news/best-worst-questions-congress-google-2018-12

Cawley, C. (2018b, Oct 15). Politicians Are Too Out of Touch to Make Laws About Tech. Retrieved from https://tech.co/news/politicians-out-of-touch-laws-regulate-tech-2018-10

CDT. (2013, July 18). Joint Transparency Letter. Retrieved from https://www.cdt.org/files/pdfs/weneedtoknow-transparency-letter.pdf

CDT. (2014, July 30). Microsoft Ireland Case: Can a US Warrant Compel A US Provider to Disclose Data Stored Abroad? Retrieved from https://cdt.org/insight/microsoft-ireland-case-can-a-us-warrant-compel-a-us-provider-to-disclose-data-stored-abroad/

CEBR. (2010). *THE CLOUD DIVIDEND Part One: The economic benefits of cloud computing to business and the wider EMEA economy* Retrieved from http://www.redstor.com/downloads/cloud-dividend-report.pdf

CEBR. (2011). *THE CLOUD DIVIDEND Part Two: The economic benefits of cloud computing to business and the wider EMEA economy* Retrieved from http://www.globbtv.com/microsite/35/Adjuntos/CLOUD-DIVIDEND-REPORT.PDF

Celuch, K., Bantham, J. H., & Kasouf, C. J. (2011). The role of trust in buyer–seller conflict management. *Journal of Business Research, 64*(10), 1082-1088.

Chaffin, J. (2013, July 19). EU to review 'safe harbour' data privacy rule for US companies. Retrieved from http://www.ft.com/cms/s/0/285454b4-f091-11e2-929c-00144feabdc0.html

Chahal, R. K., & Singh, S. (2017). Fuzzy rule-based expert system for determining trustworthiness of cloud service providers. *International Journal of Fuzzy Systems, 19*(2), 338-354.

Chakraborty, S., & Roy, K. (2012, June 25-27). *An SLA-based Framework for Estimating Trustworthiness of a Cloud.* Paper presented at the 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications.

Chao, G. T., & Moon, H. (2005). The cultural mosaic: A metatheory for understanding the complexity of culture. *Journal of Applied Psychology, 90*(6), 1128.

Charmaz, K. (2014). *Constructing Grounded Theory*: SAGE Publications.

Chaudhuri, A., & Holbrook, M. B. (2001). The chain of effects from brand trust and brand affect to brand performance: the role of brand loyalty. *Journal of Marketing, 65*(2), 81-93.

Chazan, G. (2017, January 25). Why Germany needs to accelerate into the digital fast lane. Retrieved from https://www.ft.com/content/31469796-dcd1-11e6-9d7c-be108f1c1dce

Chen, Y., Paxson, V., & Katz, R. H. (2010). What's new about cloud computing security? *University of California, Berkeley Report No. UCB/EECS-2010-5 January, 20*(2010), 2010-2015.

Cheung, A. S. Y., & Weber, R. H. (2015). *Privacy and Legal Issues in Cloud Computing*: Edward Elgar Publishing, Incorporated.

Chiasson, M., Henfridsson, O., Karsten, H., & DeGross, J. I. (2011). *Researching the Future in Information Systems: IFIP WG 8.2 Working Conference, Future IS 2011, Turku, Finland, June 6-8, 2011, Proceedings*: Springer Berlin Heidelberg.

Child, J. (2001). Trust--The Fundamental Bond in Global Collaboration. *Organizational Dynamics, 29*(4), 274-288.

Child, J. T., & Starcher, S. C. (2016). Fuzzy Facebook privacy boundaries: Exploring mediated lurking, vague-booking, and Facebook privacy management. *Computers in Human Behavior, 54*, 483-490.

Chiregi, M., & Navimipour, N. J. (2016). A new method for trust and reputation evaluation in the cloud environments using the recommendations of opinion leaders' entities and removing the effect of troll entities. *Computers in Human Behavior, 60*, 280-292. doi:10.1016/j.chb.2016.02.029

Chiregi, M., & Navimipour, N. J. (2017). A comprehensive study of the trust evaluation mechanisms in the cloud computing. *Journal of Service Science Research, 9*(1), 1-30.

Chiu, C.-M., Hsu, M.-H., Lai, H., & Chang, C.-M. (2012). Re-examining the influence of trust on online repeat purchase intention: The moderating role of habit and its antecedents. *Decision Support Systems, 53*(4), 835-845.

Chiu, C.-M., Huang, H.-Y., & Yen, C.-H. (2010). Antecedents of trust in online auctions. *Electronic Commerce Research and Applications, 9*(2), 148-159.

Chong, S.-K., Abawajy, J., Ahmad, M., & Hamid, I. R. A. (2014). Enhancing Trust Management in Cloud Environment. *Procedia - Social and Behavioral Sciences, 129*, 314-321. doi:10.1016/j.sbspro.2014.03.682

Chow, S., & Holden, R. (1997). Toward An Understanding Of Loyalty: The Moderating Role Of Trust. *Journal of Managerial Issues, 9*(3), 275-298. doi:10.2307/40604148

CIGI-Ipsos. (2014). 2014 CIGI-Ipsos Global Survey on Internet Security and Trust. Retrieved from https://www.cigionline.org/sites/default/files/documents/internet-survey-2014-slides.pdf

Cisco. (2009). Cisco Cloud Computing - Data Center Strategy, Architecture, and Solutions. *Cisco Systems, Inc. .* Retrieved from http://www.cisco.com/web/strategy/docs/gov/CiscoCloudComputing_WP.pdf

Citrin, J., & Stoker, L. (2018). Political trust in a cynical age. *Annual Review of Political Science, 21*, 49-70.

Citrix. (2012). The top 5 truths behind what the cloud is not -- Separating the noise of what cloud is and what it's not. *Citrix Systems, Inc. .* Retrieved from http://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/the-top-5-truths-behind-what-the-cloud-is-not.pdf

CJEU. (2015, October 6). Judgment of the Court (Grand Chamber) of 6 October 2015: Maximillian Schrems v Data Protection Commissioner. Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1444299455884&uri=CELEX:62014CJ0362

Clough, P., & Nutbrown, C. (2012). *A Student's Guide to Methodology*: SAGE Publications.

Coldwell, D., & Herbst, F. (2004). *Business Research*: Juta Academic.

Coles, C. (2014). Only 1 in 100 Cloud Providers Meet Proposed EU Data Protection Requirements. Retrieved from https://www.skyhighnetworks.com/cloud-security-blog/only-1-in-100-cloud-providers-meet-proposed-eu-data-protection-requirements/

Colley, A., & Maltby, J. (2008). Impact of the Internet on our lives: Male and female personal perspectives. *Computers in Human Behavior, 24*(5), 2005-2013.

Collins, C. J., & Smith, K. G. (2006). Knowledge exchange and combination: The role of human resource practices in the performance of high-technology firms. *Academy of Management Journal, 49*(3), 544-560.

Collins, H. (2010). *Creative Research: The Theory and Practice of Research for the Creative Industries*: AVA Publishing.

Columbus, L. (2013, March 12). Why Cloud Computing Is Slowly Winning The Trust War. *Forbes*. Retrieved from http://www.forbes.com/sites/louiscolumbus/2013/03/12/why-cloud-computing-is-slowly-winning-the-trust-war/

Computerwoche. (2012, March 26). Cloud-Services aus Deutschland [Cloud services from Germany]. Retrieved from http://www.computerwoche.de/a/cloud-services-aus-deutschland,2359614

Computerwoche. (2013, June 26). Überwachungsskandal erschüttert Vertrauen in Internet-Dienste [Surveillance scandal shakes trust in Internet services]. Retrieved from http://www.computerwoche.de/2541286

Connolly, C. (2008). The US Safe Harbor - Fact or Fiction? Retrieved from http://www.galexia.com/public/research/assets/trustmarks_struggle_20080926/trustmarks_struggle_public.pdf

Cooper, H. M. (1984). *The integrative research review: a systematic approach*: Sage Publications.

Coote, L. V., Forrest, E. J., & Tam, T. W. (2003). An investigation into commitment in non-Western industrial marketing relationships. *Industrial Marketing Management, 32*(7), 595-604.

Corbin, J., & Strauss, A. (2014). *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*: SAGE Publications.

Corporate Trust. (2014). *Studie: Industriespionage 2014 [Study: industrial espionage in 2014]* Retrieved from https://www.corporate-trust.de/wp-content/uploads/2016/06/CT-Studie-2014_DE.pdf

Corritore, C. L., Kracher, B., & Wiedenbeck, S. (2003). On-line trust: concepts, evolving themes, a model. *International Journal of Human-Computer Studies, 58*(6), 737-758. doi:10.1016/S1071-5819(03)00041-7

Council of Europe. (1950). *Convention for the Protection of Human Rights and Fundamental Freedoms*. Rome Retrieved from http://www.echr.coe.int/Documents/Convention_ENG.pdf.

Cowles, D. L., Kiecker, P., & Little, M. W. (2002). Using key informant insights as a foundation for e-retailing theory development. *Journal of Business Research, 55*(8), 629-636.

Creswell, J. W. (2007). *Qualitative Inquiry and Research Design: Choosing Among Five Approaches*: SAGE Publications.

Creswell, J. W. (2013). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*: SAGE Publications.

Croft, A. (2013, July 5). EU threatens to suspend data-sharing with U.S. over spy reports. Retrieved from http://www.reuters.com/article/us-usa-security-eu-idUSBRE9640JJ20130705

Cron, W. L., Marshall, G. W., Singh, J., Spiro, R. L., & Sujan, H. (2005). Salesperson selection, training, and development: Trends, implications, and research opportunities. *Journal of Personal Selling & Sales Management, 25*(2), 123-136.

Crosby, L. A., Evans, K. R., & Cowles, D. (1990). Relationship quality in services selling: an interpersonal influence perspective. *The Journal of Marketing*, 68-81.

CSA. (2011). *Security Guidance for Critical Areas of Focus in Cloud Computing Version 3* Retrieved from http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

CSA. (2013). Government Access to Information Survey Results, July 2013. *Cloud Security Alliance (CSA).* Retrieved from https://downloads.cloudsecurityalliance.org/initiatives/surveys/nsa_prism/CSA-govt-access-survey-July-2013.pdf

Cunliffe, A. L. (2003). Reflexive inquiry in organizational research: Questions and possibilities. *Human Relations, 56*(8), 983-1003.

Curry, A. (2015, January 14). No, the NSA Isn't Like the Stasi—And Comparing Them Is Treacherous. Retrieved from https://www.wired.com/2015/01/nsa-stasi-comparison/

Curtis, S. (2014, March 3). Salesforce to open three data centres in Europe. Retrieved from http://www.telegraph.co.uk/technology/news/10667686/Salesforce-to-open-three-data-centres-in-Europe.html

Czarniawska, B. (2003). Forbidden knowledge: Organization theory in times of transition. *Management learning, 34*(3), 353-365.
Czarniawska, B. (2014). *Social Science Research: From Field to Desk*: SAGE Publications.
D'Arcy, P. (2011). CIO strategies for consumerization: the future of enterprise mobile computing *Dell CIO Insight Series* (pp. 1-15): Dell Inc.
Darrow, B. (2012, January 17). Buckle up for a new wave of cloud protectionism. Retrieved from http://gigaom.com/2012/01/17/buckle-up-for-a-new-wave-of-cloud-protectionism/
Dasí-Rodríguez, S., & Pardo-del-Val, M. (2015). Seeking partners in international alliances: The influence of cultural factors. *Journal of Business Research, 68*(7), 1522-1526. doi:10.1016/j.jbusres.2015.01.045
Davies, R. (2019). Jeff Bezos: the Amazon billionaire and Trump bete noire. Retrieved from https://www.theguardian.com/technology/2019/feb/08/jeff-bezos-the-man-behind-the-amazon-phenomenon
Davis, S., Brodersen, S., Böhmer, G., & Siemens, A. (2017). Digitalization sparks a quiet revolution. *World Pumps, 2017*(5), 28-31.
Dearden, L. (2014, July 5). 'Double agent' arrested in Germany for passing information on NSA inquiry to the US. Retrieved from http://www.independent.co.uk/news/world/europe/suspected-spy-arrested-in-germany-for-passing-us-information-on-nsa-inquiry-9586360.html
DeCarlo, T. E. (2005). The effects of sales message and suspicion of ulterior motives on salesperson evaluation. *Journal of Consumer Psychology, 15*(3), 238-249.
Delgado-Ballester, E., & Luis Munuera-Alemán, J. (2001). Brand trust in the context of consumer loyalty. *European Journal of Marketing, 35*(11/12), 1238-1258.
Deloitte. (2011). *Cloud Computing in Deutschland*. Retrieved from http://www.deloitte.com/view/de_DE/de/branchen/technology-media-telecommunications/technologyfast50/47a8f3a12ed9d210VgnVCM3000001c56f00aRCRD.htm#
Delvecchio, S., Zemanek, J., McIntyre, R., & Claxton, R. (2004). Updating the adaptive selling behaviours: tactics to keep and tactics to discard. *Journal of Marketing Management, 20*(7-8), 859-875.
Dempsey, D., & Kelliher, F. (2017). *Industry Trends in Cloud Computing: Alternative Business-to-Business Revenue Models*: Springer International Publishing.
Denzin, N. K., & Lincoln, Y. S. (2011). *The SAGE Handbook of Qualitative Research*: SAGE Publications.
Der Tagesspiegel. (2012, March 4). Bitkom-Präsident Kempf: Sicherheit ist eine Frage des Preises [Bitkom President Kempf: Security is a matter of price]. Retrieved from http://www.tagesspiegel.de/wirtschaft/bitkom-praesident-kempf-sicherheit-ist-eine-frage-des-preises/6283470.html
DeSantis, L., & Ugarriza, D. N. (2000). The concept of theme as used in qualitative nursing research. *Western Journal of Nursing Research, 22*(3), 351-372.
Dess, G. G., & Beard, D. W. (1984). Dimensions of organizational task environments. *Administrative science quarterly*, 52-73.
Destatis. (2017). Imports and exports (special trade) by division of the national Product Classification for Production Statistics 2016. Retrieved from https://www.destatis.de/EN/FactsFigures/NationalEconomyEnvironment/ForeignTrade/Tables/ImportsExports.html
Deutsch, M. (1958). Trust and suspicion. *The Journal of Conflict Resolution (pre-1986), 2*(4), 265.
Deutsch, M. (1960). The effect of motivational orientation upon trust and suspicion. *Human Relations, 13*(2), 123-139.
Deutsche Welle. (2013a, October 24). German foreign minister summons US ambassador over Merkel spying allegations. Retrieved from http://www.dw.com/en/german-

foreign-minister-summons-us-ambassador-over-merkel-spying-allegations/a-17180294
Deutsche Welle. (2013b, July 17). Itching to ask: What does Merkel know about NSA surveillance? Retrieved from http://www.dw.com/en/itching-to-ask-what-does-merkel-know-about-nsa-surveillance/a-16957061
Deutsche Welle. (2013c, October 23). Merkel presses Obama for answers over allegation US spied on her cellphone. Retrieved from http://www.dw.com/en/merkel-presses-obama-for-answers-over-allegation-us-spied-on-her-cellphone/a-17179704
Deutsche Welle. (2016, April 21). TTIP skepticism grows in Germany and the US. Retrieved from http://www.dw.com/en/ttip-skepticism-grows-in-germany-and-the-us/a-19203036
Dhont, J., Asinari, M. V. P., & Poullet, Y. (2004). *Safe Harbour Decision Implementation Study*. Retrieved from
DiCicco-Bloom, B., & Crabtree, B. F. (2006). The qualitative research interview. *Medical Education, 40*(4), 314-321. doi:10.1111/j.1365-2929.2006.02418.x
Dieckmann, F. (2013, October 26). Ausspähaffäre: Deutsche Industrie fordert Ächtung von Wirtschaftsspionage [Spying affair: German industry calls for ostracism of economic espionage]. Retrieved from http://www.spiegel.de/wirtschaft/soziales/spaehaffaere-bdi-chef-grillo-fordert-aechtung-von-wirtschaftsspionage-a-930092.html
Dietz, G., & Gillespie, N. (2012). *Recovery of Trust: Case Studies of Organisational Failures and Trust Repair* (Vol. 5): Institute of Business Ethics.
Dietz, G., Gillespie, N., & Chao, G. T. (2010). Unravelling the complexities of trust and culture. In M. N. K. Saunders, D. Skinner, G. Dietz, N. Gillespie, & R. J. Lewicki (Eds.), *Organizational trust: A cultural perspective* (pp. 3-41).
Dimensional Research. (2017). Privacy and the EU GDPR: 2017 Survey of Privacy Professionals. Retrieved from https://download.trustarc.com/dload.php/?f=JT190EEP-669
Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., & Colautti, C. (2006). Privacy calculus model in e-commerce–a study of Italy and the United States. *European Journal of Information Systems, 15*(4), 389-402.
Dinev, T., Goo, J., Hu, Q., & Nam, K. (2009). User behaviour towards protective information technologies: the role of national cultural differences. *Information systems journal, 19*(4), 391-412.
Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17*(1), 61-80.
Dirks, K. T., Kim, P. H., Ferrin, D. L., & Cooper, C. D. (2011). Understanding the effects of substantive responses on trust following a transgression. *Organizational behavior and human decision processes, 114*(2), 87-103.
Dix, A., Thüsing, G., Traut, J., Christensen, L., Etro, F., Aaronson, S., & Maxim, R. (2013). EU data protection reform: Opportunities and concerns. *Intereconomics, 48*(5), 268-285. doi:10.1007/s10272-013-0470-y
Doe v. Ashcroft, United States District Court, 334 F. SUPP. 2D 471 S.D.N.Y., (2004).
Doe v. Ganzales, United States District Court, 500 F. SUPP. 2D 379 S.D.N.Y., (2007).
DOJ. (2007). A Review of the Federal Bureau of Investigation's Use of National Security Letters. *U. S. Department of Justice: Office of the Inspector General.* Retrieved from http://www.justice.gov/oig/special/s0703b/final.pdf
Domnik, J. (2015, May 12). Private oder Public Cloud – welche Lösung am besten passt. Retrieved from http://www.computerwoche.de/a/private-oder-public-cloud-welche-loesung-am-besten-passt,3099017
Donegan, M. (2014). Deutsche Telekom Aims for Security Advantage. Retrieved from http://www.lightreading.com/mobile/mobile-security/deutsche-telekom-aims-for-security-advantage/d/d-id/708660?_mc=RSS_LR_EDT

Doney, P. M., Barry, J. M., & Abratt, R. (2007). Trust determinants and outcomes in global B2B services. *European Journal of Marketing, 41*(9/10), 1096-1116.
Doney, P. M., & Cannon, J. P. (1997). An examination of the nature of trust in buyer-seller relationships. *The Journal of Marketing*, 35-51.
Doney, P. M., Cannon, J. P., & Mullen, M. R. (1998). Understanding the influence of national culture on the development of trust. *Academy of management review, 23*(3), 601-620.
Donnelley, C. (2015, October 9). EU Data Protection Regulation: What the EC legislation means for cloud providers. Retrieved from http://www.computerweekly.com/feature/EU-Data-Protection-Regulation-What-the-EC-legislation-means-for-cloud-providers
Donohue, L. (2015). High Technology, Consumer Privacy, and US National Security. *Am. U. Bus. L. Rev., 4*, 11.
Dowell, D., Heffernan, T., & Morrison, M. (2013). Trust formation at the growth stage of a business-to-business relationship: a qualitative investigation. *Qualitative Market Research: An International Journal, 16*(4), 436-451.
Doyle, C. (2002). *The USA PATRIOT Act: A Legal Analysis* (Order Code RL31377), Retrieved from http://www.fas.org/irp/crs/RL31377.pdf
Doyle, C. (2014, January 3). National Security Letters in Foreign Intelligence Investigations: Legal Background *Congressional Research Service Report Prepared for Members and Committees of Congress.* Retrieved from https://www.fas.org/sgp/crs/intel/RL33320.pdf
Dropbox. (2016a, February 11). Dropbox is growing in Europe. Retrieved from https://blogs.dropbox.com/business/2016/02/dropbox-is-growing-in-europe/
Dropbox. (2016b, May 23). Moin moin, Hamburg: It's Dropbox. Retrieved from https://blogs.dropbox.com/dropbox/2016/05/moin-moin-hamburg
Dutta, A., Peng, G. C. A., & Choudhary, A. (2013). Risks in enterprise cloud computing: The perspective of IT experts. *The Journal of Computer Information Systems, 53*(4), 39-48. doi:10.1109/CLOUD.2009.5071532
Dutton, W. H. (2013). *The Oxford Handbook of Internet Studies*: OUP Oxford.
Dwyer, F. R., Schurr, P. H., & Oh, S. (1987). Developing buyer-seller relationships. *The Journal of Marketing*, 11-27.
Dyer, J. H., & Chu, W. (2000). The Determinants of Trust in Supplier-Automaker Relationships in the U.S., Japan, and Korea. *Journal of international Business studies, 31*(2), 259-285. doi:10.2307/155637
Dyer, J. H., & Chu, W. (2003). The Role of Trustworthiness in Reducing Transaction Costs and Improving Performance: Empirical Evidence from the United States, Japan, and Korea. *Organization Science, 14*(1), 57-68. doi:10.2307/3086033
Easterby-Smith, M., Thorpe, R., & Jackson, P. R. (2008). *Management Research: Third Edition*: SAGE.
Easterby-Smith, M., Thorpe, R., & Lowe, A. (2002). *Management research: an introduction*: SAGE.
Eastlick, M. A., Lotz, S. L., & Warrington, P. (2006). Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment. *Journal of Business Research, 59*(8), 877-886.
Easton, G. (2010). Critical realism in case study research. *Industrial Marketing Management, 39*(1), 118-128.
Edgar, A., & Sedgwick, P. R. (2008). *Cultural theory: the key concepts*: Routledge.
EFF. (2014, March 3). EFF Fights National Security Letter Demands on Behalf of Telecom, Internet Company. *Electronic Frontier Foundation.* Retrieved from https://www.eff.org/press/releases/eff-fights-national-security-letter-demands-behalf-telecom-internet-company
EFF. (2015). PATRIOT Act. Retrieved from https://www.eff.org/issues/patriot-act

Eggen, D. (2007, September 7). Judge Invalidates Patriot Act Provisions. *The Washington Post.* Retrieved from http://www.washingtonpost.com/wp-dyn/content/article/2007/09/06/AR2007090601438_pf.html

Eisenhardt, K. M. (1989). Building theories from case study research. *Academy of management review, 14*(4), 532-550.

El-Gazzar, R. (2016). Understanding the Phenomenon of Cloud Computing Adoption within Organizations.

El-Gazzar, R., Hustad, E., & Olsen, D. H. (2016). Understanding cloud computing adoption issues: A Delphi study approach. *Journal of Systems and Software, 118*, 64-84. doi:10.1016/j.jss.2016.04.061

Emeakaroha, V. C., Fatema, K., van der Werff, L., Healy, P., Lynn, T., & Morrison, J. P. (2017). A trust label system for communicating trust in cloud services. *IEEE Transactions on Services Computing, 10*(5), 689-700.

Enderle, R. (2015, June 12). U.S. surveillance programs are killing the tech industry. Retrieved from http://www.cio.com/article/2934887/privacy/u-s-surveillance-programs-are-killing-the-tech-industry.html

ENISA. (2009). Cloud Computing -- Benefits, risks and recommendations for information security. *European Network and Information Security Agency (ENISA).* Retrieved from https://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport.

ENISA. (2013). Good Practice Guide for securely deploying Governmental Clouds. *European Network and Information Security Agency (ENISA).* Retrieved from http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/good-practice-guide-for-securely-deploying-governmental-clouds/at_download/fullReport

Enli, G., & Rosenberg, L. T. (2018). Trust in the age of social media: populist politicians seem more authentic. *Social Media+ Society, 4*(1), 2056305118764430.

EPIC. (2015). USA Patriot Act. Retrieved from https://epic.org/privacy/terrorism/usapatriot/

Erl, T., Puttini, R., & Mahmood, Z. (2013). *Cloud Computing: Concepts, Technology & Architecture*: Pearson Education.

Ermakova, T., Huenges, J., Erek, K., & Zarnekow, R. (2013). Cloud Computing in Healthcare–A literature review on current state of research.

Ertaul, L., Singhal, S., & Saldamli, G. (2010). *Security Challenges in Cloud Computing.* Paper presented at the Security and Management.

Ess, C., & Sudweeks, F. (2005). Culture and computer-mediated communication: Toward new understandings. *Journal of Computer-Mediated Communication, 11*(1), 9.

Etherington, D. (2017, January 30). Amazon, Expedia and Microsoft to support Washington state lawsuit on Trump immigration order. Retrieved from https://techcrunch.com/2017/01/30/amazon-and-expedia-to-support-washington-state-lawsuit-on-trump-immigration-order/

European Commission. (1995). *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*. THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION.

European Commission. (2000). Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce. *European Commission.* Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML

European Commission. (2002). *The application of Commission Decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequate protection of personal data provided by the Safe Harbour Privacy*

Principles and related Frequently Asked Questions issued by the US Department of Commerce. (SEC(2002) 196). Brussels: European Commission.

European Commission. (2004). *The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce*. (SEC (2004) 1323). Brussels: European Commission.

European Commission. (2009). *Frequently asked questions relating to transfers of personal data from the EU/EEA to third countries* Retrieved from http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf

European Commission. (2012a, January 25). Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses. Retrieved from http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en

European Commission. (2012b, October 9). How will the "safe harbor" arrangement for personal data transfers to the US work? Retrieved from http://ec.europa.eu/justice/policies/privacy/thridcountries/adequacy-faq1_en.htm

European Commission. (2012c). *Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Up-take (SMART 2011/0045)* Retrieved from http://ec.europa.eu/information_society/activities/cloudcomputing/docs/quantitative_estimates.pdf

European Commission. (2012d). *Unleashing the Potential of Cloud Computing in Europe* Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF

European Commission. (2012e). Unleashing the Potential of Cloud Computing in Europe - What is it and what does it mean for me? MEMO/12/713 [Press release]. Retrieved from http://europa.eu/rapid/press-release_MEMO-12-713_en.htm

European Commission. (2013a, Jun 18). COMMISSION DECISION of 18 June 2013 on setting up the Commission expert group on cloud computing contracts. Retrieved from https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2013:174:0006:0008:EN:PDF

European Commission. (2013b). *Communication on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Establsiehd in the EU* Retrieved from http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf

European Commission. (2013c, November 27). European Commission calls on the U.S. to restore trust in EU-U.S. data flows. *European Commission - IP/13/1166.* Retrieved from http://europa.eu/rapid/press-release_IP-13-1166_en.htm

European Commission. (2013d, November 27). Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection. *European Commission.* Retrieved from http://ec.europa.eu/justice/data-protection/files/report-findings-of-the-ad-hoc-eu-us-working-group-on-data-protection.pdf

European Commission. (2013e, November 27). Restoring Trust in EU-US data flows - Frequently Asked Questions. *European Commission - MEMO/13/1059.* Retrieved from http://europa.eu/rapid/press-release_MEMO-13-1059_en.htm

European Commission. (2013f, July 4). Statement by Vice President Neelie Kroes "on the consequences of living in an age of total information" MEMO/13/654. *European Commission.* Retrieved from http://europa.eu/rapid/press-release_MEMO-13-654_en.htm

European Commission. (2015a, November 6). COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14

(Schrems). Retrieved from http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/files/eu-us_data_flows_communication_final.pdf

European Commission. (2015b). *Uptake of Cloud in Europe - Follow-up of IDC Study on Quantitative estimates of the demand for Cloud Computing in Europe and the likely barriers to take-up*: European Commission.

European Commission. (2015c). What is an SME? Retrieved from http://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition/index_en.htm

European Commission. (2016, February 29). Transatlantic Data Flows: Restoring Trust through Strong Safeguards. Retrieved from http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-communication_en.pdf

European Commission. (2017, Oct 18). EU-U.S. Privacy Shield: First review shows it works but implementation can be improved. Retrieved from http://europa.eu/rapid/press-release_IP-17-3966_en.htm

European Council. (2013, October 25). EUROPEAN COUNCIL 24/25 October 2013 Conclusions. Retrieved from http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/139197.pdf

European Parliament. (1995). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *European Parliament.* Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046

European Parliament. (2012). Fighting cyber crime and protecting privacy in the cloud. *European Parliament's Committee on Civil Liberties, Justice and Home Affairs.* Retrieved from http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/462509/IPOL-LIBE_ET(2012)462509_EN.pdf

European Parliament. (2013). The US surveillance programmes and their impact on EU citizens' fundamental rights. *European Parliament.* Retrieved from http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/briefingnote_/briefingnote_en.pdf

European Parliament. (2014a, February 21). Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs. Retrieved from http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A7-2014-0139&language=EN

European Parliament. (2014b, March 13). US NSA: stop mass surveillance now or face consequences, MEPs say. *European Parliament, Committees Committee on Civil Liberties, Justice and Home Affairs Plenary sessions [12-03-2014 - 12:51].* Retrieved from http://www.europarl.europa.eu/pdfs/news/expert/infopress/20140307IPR38203/20140307IPR38203_en.pdf

European Parliament. (2016). General Data Protection Regulation. *(EU) 2016/679.* Retrieved from http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679

Eurostat. (2017, Mar 30). Cloud computing use in EU enterprises. Retrieved from http://ec.europa.eu/eurostat/web/products-eurostat-news/-/DDN-20170330-1

Evans, K. R., McFarland, R. G., Dietz, B., & Jaramillo, F. (2012). Advancing sales performance research: A focus on five underresearched topic areas. *Journal of Personal Selling & Sales Management, 32*(1), 89-105.

Everett, C. (2009). Cloud computing – A question of trust. *Computer Fraud & Security, 2009*(6), 5-7. doi:10.1016/S1361-3723(09)70071-5

Ewing, J., & Scott, M. (2017, February 8). German Automakers Step Up to Silicon Valley Challenge. Retrieved from https://www.nytimes.com/2017/02/08/business/germany-bmw-daimler-volkswagen-uber.html

Exact. (2016, June 28). KMU Barometer 2016: Deutschland holt bei CloudNutzung stark auf – bleibt aber internationales Schlusslicht [SME barometer 2016: Germany is catching up strongly with the use of the cloud - but remains the international backlit].

Experton. (2012). *Cloud Vendor Benchmark 2012*. Retrieved from http://www.experton-group.de/research/studien/cloud-vendor-benchmark-2012.html

Experton. (2014). *Cloud Vendor Benchmark 2014*. Retrieved from http://www.experton-group.de/research/studien/cloud-vendor-benchmark-2014.html

EY. (2013, August 5). Deutsche Unternehmen fürchten Cyber-Attacken aus China und den USA [German companies fear cyber attacks from China and the USA]. Retrieved from http://www.ey.com/DE/de/Newsroom/News-releases/20130802-Datenklau---Neue-Herausforderungen-fuer-deutsche-Unternehmen

Fan, W., & Perros, H. (2014). A novel trust management framework for multi-cloud environments based on trust service providers. *Knowledge-Based Systems, 70*, 392-406. doi:10.1016/j.knosys.2014.07.018

Fang, E., Palmatier, R. W., Scheer, L. K., & Li, N. (2008). Trust at different organizational levels. *Journal of Marketing, 72*(2), 80-98.

Farris, G. F., Senner, E. E., & Butterfield, D. A. (1973). Trust, culture, and organizational behavior. *Industrial Relations: A Journal of Economy and Society, 12*(2), 144-157.

Faynberg, I., Lu, H. L., & Skuler, D. (2016). *Cloud Computing: Business Trends and Technologies*: Wiley.

Feinstein, D. (2013, October 28). Feinstein Statement on Intelligence Collection of Foreign Leaders. *United States Senator for California.* Retrieved from http://www.feinstein.senate.gov/public/index.cfm/2013/10/feinstein-statement-on-intelligence-collection-of-foreign-leaders

Ferrin, D. L., & Gillespie, N. (2010). Trust differences across national-societal cultures: Much to do, or much ado about nothing. *Organizational trust: A cultural perspective*, 42-86.

Fersch, B. (2012). 'German Angst' vs 'Danish Easy-going'? On the Role and Relevance of Insecurity and Uncertainty in the Lives of Freelancers in Denmark and Germany. *Sociology, 46*(6), 1125-1139. doi:10.1177/0038038512437894

Fisher, K. (2003). Demystifying critical reflection: Defining criteria for assessment. *Higher Education Research & Development, 22*(3), 313-325.

Fisher, M. (2013, June 11). Germans so outraged at U.S. over spying that Merkel will raise the issue directly with Obama. Retrieved from https://www.washingtonpost.com/news/worldviews/wp/2013/06/11/germans-so-outraged-at-u-s-over-spying-that-merkel-will-raise-the-issue-directly-with-obama/

Flamez, B., Lenz, A. S., Balkin, R. S., & Smith, R. L. (2017). *A Counselor's Guide to the Dissertation Process: Where to Start and How to Finish*: Wiley.

Flick, U. (2014). *An Introduction to Qualitative Research*: SAGE Publications.

Flick, U., Kvale, S., Angrosino, M. V., Barbour, R. S., Banks, M., Gibbs, G., & Rapley, T. (2007). *Designing Qualitative Research*: SAGE.

Flick, U., von Kardoff, E., Steinke, I., & Jenner, B. (2004). *A Companion to Qualitative Research*: SAGE Publications.

Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior, 25*(1), 153-160.

Follorou, J. (2016, December 7). American and British spy agencies targeted in-flight mobile phone use. Retrieved from https://theintercept.com/2016/12/07/american-and-british-spy-agencies-targeted-in-flight-mobile-phone-use/

Ford, D. (1984). Buyer/seller relationships in international industrial markets. *Industrial Marketing Management, 13*(2), 101-112. doi:10.1016/0019-8501(84)90041-5

Ford, D. P., Connelly, C. E., & Meister, D. B. (2003). Information systems research and Hofstede's culture's consequences: an uneasy and incomplete partnership. *IEEE Transactions on Engineering Management, 50*(1), 8-25.

Forrester. (2013). Cloud Computing. *Forrester Research, Inc.* Retrieved from http://www.forrester.com/Cloud-Computing

Forrester. (2016, November 9). Forrester Data: Public Cloud Services Forecast, 2016 To 2020 (Global). Retrieved from https://www.forrester.com/report/Forrester+Data+Public+Cloud+Services+Forecast+2016+To+2020+Global/-/E-RES136524

Forrester. (2017). Privacy and data protection by country. Retrieved from http://heatmap.forrestertools.com/

Foster, I., Zhao, Y., Raicu, I., & Lu, S. (2008). *Cloud computing and grid computing 360-degree compared.* Paper presented at the Grid Computing Environments Workshop, 2008. GCE'08.

Foster, T. N. (2013). Navigating through the fog of cloud computing contracts. *J. Marshall J. Info. Tech. & Privacy L., 30*, 13.

Francisco, A., Jack, S., Joana, A., & Juan, M. (2017). Innovation through Shadow IT.

Franke, G. R., & Park, J.-E. (2006). Salesperson adaptive selling behavior and customer orientation: a meta-analysis. *Journal of marketing research, 43*(4), 693-702.

Freris, N. M., & Patrinos, P. (2016). *Distributed computing over encrypted data.* Paper presented at the 2016 54th Annual Allerton Conference on Communication, Control, and Computing (Allerton).

Friedlander, F. (1970). The primacy of trust as a facilitator of further group accomplishment. *The Journal of Applied Behavioral Science, 6*(4), 387-400.

Friend, S. B., Johnson, J. S., & Sohi, R. S. (2018). Propensity to trust salespeople: A contingent multilevel-multisource examination. *Journal of Business Research, 83*, 1-9.

Friman, M., Gärling, T., Millett, B., Mattsson, J., & Johnston, R. (2002). An analysis of international business-to-business relationships based on the Commitment–Trust theory. *Industrial Marketing Management, 31*(5), 403-409. doi:10.1016/S0019-8501(01)00154-7

Frost, T., Stimpson, D. V., & Maughan, M. R. (1978). Some correlates of trust. *Journal of Psychology: Interdisciplinary and Applied, 99*(1), 103-108. doi:10.1080/00223980.1978.9921447

Fu, Z., Sun, X., Liu, Q., Zhou, L., & Shu, J. (2015). Achieving efficient cloud search services: multi-keyword ranked search over encrypted cloud data supporting parallel computing. *IEICE Transactions on Communications, 98*(1), 190-200.

Fukuyama, F. (1995). *Trust: the social virtues and the creation of prosperity*: Free Press Paperbacks.

Fürstenau, D., Rothe, H., & Sandner, M. (2017). Shadow systems, risk, and shifting power relations in organizations. *Communications of the Association for Information Systems, 41*(1), 3.

Gallagher, R. (2014, August 25). The Surveillance Engine - How the NSA Built Its Own Secret Google. Retrieved from https://theintercept.com/2014/08/25/icreach-nsa-cia-secret-google-crisscross-proton/

Gallagher, R., & Greenwald, G. (2014, March 12). How the NSA Plans to Infect 'Millions' of Computers with Malware. Retrieved from https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/

Gallagher, S. (2013, December 10). NSA leaks blamed for Cisco's falling sales overseas (updated). Retrieved from http://arstechnica.com/information-technology/2013/12/nsa-leaks-blamed-for-ciscos-falling-sales-overseas/

Gallagher, S. (2014, May 14). Photos of an NSA “upgrade” factory show Cisco router getting implant. Retrieved from https://arstechnica.com/tech-policy/2014/05/photos-of-an-nsa-upgrade-factory-show-cisco-router-getting-implant/

Gallagher, S. (2018, Nov 21). The Snowden Legacy, part one: What’s changed, really? Retrieved from https://arstechnica.com/tech-policy/2018/11/the-snowden-legacy-part-one-whats-changed-really/

Gambetta, D. (1988). Can we trust trust? In D. Gambetta (Ed.), *Trust: Making and Breaking Cooperative Relations* (pp. 213-237): Department of Sociology, University of Oxford.

Ganesan, S. (1994). Determinants of long-term orientation in buyer-seller relationships. *The Journal of Marketing*, 1-19.

Ganesan, S., & Hess, R. (1997). Dimensions and levels of trust: implications for commitment to a relationship. *Marketing letters, 8*(4), 439-448.

Gannon, M. J. (2004). *Understanding Global Cultures: Metaphorical Journeys Through 28 Nations, Clusters of Nations, and Continents*: SAGE Publications.

Gao, G. (2015, May 29). What Americans think about NSA surveillance, national security and privacy. Retrieved from http://www.pewresearch.org/fact-tank/2015/05/29/what-americans-think-about-nsa-surveillance-national-security-and-privacy/

Gao, T., Sirgy, M. J., & Bird, M. M. (2005). Reducing buyer decision-making uncertainty in organizational purchasing: can supplier trust, commitment, and dependence help? *Journal of Business Research, 58*(4), 397-405. doi:10.1016/S0148-2963(03)00137-1

Garfinkel, S. (2011, October 3). The Cloud Imperative. *MIT Technology Review.* Retrieved from http://www.technologyreview.com/news/425623/the-cloud-imperative/

Garfinkel, S., & Abelson, H. (1999). *Architects of the Information Society: 35 Years of the Laboratory for Computer Science at MIT*: MIT Press.

Garrison, G., Kim, S., & Wakefield, R. L. (2012). Success factors for deploying cloud computing. *Communications of the ACM, 55*(9), 62-68.

Garside, J. (2014, June 6). Vodafone reveals existence of secret wires that allow state surveillance. Retrieved from https://www.theguardian.com/business/2014/jun/06/vodafone-reveals-secret-wires-allowing-state-surveillance

Gartner. (2008, September 29). Gartner Says Contrasting Views on Cloud Computing Are Creating Confusion. *Gartner, Inc.* Retrieved from http://www.gartner.com/newsroom/id/766215

Gartner. (2009, June 23). Gartner Highlights Five Attributes of Cloud Computing. *Gartner, Inc.* Retrieved from http://www.gartner.com/newsroom/id/1035013

Gartner. (2016, July 20). Gartner Says by 2020 "Cloud Shift" Will Affect More Than $1 Trillion in IT Spending. Retrieved from http://www.gartner.com/newsroom/id/3384720

Gartner. (2017, Oct 12). Gartner Forecasts Worldwide Public Cloud Services Revenue to Reach $260 Billion in 2017. Retrieved from https://www.gartner.com/newsroom/id/3815165

Gassenheimer, J. B., Houston, F. S., & Davis, J. C. (1998). The role of economic value, social value, and perceptions of fairness in interorganizational relationship retention decisions. *Journal of the Academy of Marketing Science, 26*(4), 322-337.

Gassenheimer, J. B., & Manolis, C. (2001). The Influence Of Product Customization And Supplier Selection On Future Intentions: The Mediating Effects Of Salesperson And Organizational Trust. *Journal of Managerial Issues, 13*(4), 418-435. doi:10.2307/40604362

Gaycken, S. (2017, February 26). Finding Germany's Role in the Digital Revolution. Retrieved from https://global.handelsblatt.com/opinion/finding-germanys-role-in-the-digital-revolution-711097

Géczy, P., Izumi, N., & Hasida, K. (2011). *Cloud services: Do risks outweigh benefits.* Paper presented at the 2011 2nd International Conference on Economics, Business and Management IPEDR.

Gefen, D., & Straub, D. (2003). Managing user trust in B2C e-services. *e-Service, 2*(2), 7-24.

Geist, A., Gjerding, S., Moltke, H., & Poitras, L. (2014, June 19). NSA 'third party' partners tap the Internet backbone in global surveillance program. Retrieved from https://www.information.dk/udland/2014/06/nsa-third-party-partners-tap-the-internet-backbone-in-global-surveillance-program

Gellman, B. (2005, November 6). The FBI's Secret Scrutiny. *The Washington Post.* Retrieved from http://www.washingtonpost.com/wp-dyn/content/article/2005/11/05/AR2005110501366_pf.html

Gellman, B., Blake, A., & Miller, G. (2013, June 9). Edward Snowden comes forward as source of NSA leaks. *The Washington Post.* Retrieved from http://www.washingtonpost.com/politics/intelligence-leaders-push-back-on-leakers-media/2013/06/09/fff80160-d122-11e2-a73e-826d299ff459_story.html

Gellman, B., & Miller, G. (2013, August 29). U.S. spy network's successes, failures and objectives detailed in 'black budget' summary. *The Washington Post.* Retrieved from http://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_story.html

Gellman, B., & Poitras, L. (2013, June 7). U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program. *The Washington Post.* Retrieved from http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html

Gellman, B., & Soltani, A. (2013a, October 14). NSA collects millions of e-mail address books globally. Retrieved from https://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html

Gellman, B., & Soltani, A. (2013b, October 30). NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say. *The Washington Post.* Retrieved from http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html

Gellman, B., & Soltani, A. (2013c, December 4). NSA tracking cellphone locations worldwide, Snowden documents show. *The Washington Post.* Retrieved from http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html

Gellman, B., & Soltani, A. (2014, March 18). NSA surveillance program reaches 'into the past' to retrieve, replay phone calls. Retrieved from http://www.washingtonpost.com/world/national-security/nsa-surveillance-program-reaches-into-the-past-to-retrieve-replay-phone-calls/2014/03/18/226d2646-ade9-11e3-a49e-76adc9210f19_story.html

Gellman, B., Soltani, A., & Peterson, A. (2013, November 4). How we know the NSA had access to internal Google and Yahoo cloud data [Web log post]. *The Washington Post*. Retrieved from http://www.washingtonpost.com/blogs/the-switch/wp/2013/11/04/how-we-know-the-nsa-had-access-to-internal-google-and-yahoo-cloud-data/

Germany. (1949). *Basic Law for the Federal Republic of Germany*. Bonn am Rhein Retrieved from http://www.gesetze-im-internet.de/englisch_gg/englisch_gg.html.

Germany. (1998). German Criminal Code. Retrieved from http://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html

Germany. (2003). Federal Data Protection Act in the version promulgated on 14 January 2003 (Federal Law Gazette I p. 66), as most recently amended by Article 1 of the Act of 14 August 2009 (Federal Law Gazette I p. 2814). *Federal Republic of Germany.* Retrieved from http://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html

Germany. (2011, August 22). Definition Kritische Infrastrukturen [Definition Critical Infrastructures]. Retrieved from http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/Sicherheit/BevoelkerungKrisen/Sektoreneinteilung.pdf

Gershman, J. (2013, June 6). How The Government Justifies Surveillance. Retrieved from http://blogs.wsj.com/law/2013/06/06/how-the-government-justifies-surveillance/

Geyskens, I., Steenkamp, J.-B. E. M., & Kumar, N. (1998). Generalizations about trust in marketing channel relationships using meta-analysis. *International Journal of Research in Marketing, 15*(3), 223-248. doi:http://dx.doi.org/10.1016/S0167-8116(98)00002-0

Geyskens, I., Steenkamp, J.-B. E. M., Scheer, L. K., & Kumar, N. (1996). The effects of trust and interdependence on relationship commitment: A trans-Atlantic study. *International Journal of Research in Marketing, 13*(4), 303-317.

Gibb, J. R. (1964). Climate for trust formation. *T-group theory and laboratory method, 1694*, 279-301.

Gibbs, S. (2014, October 27). Elon Musk: artificial intelligence is our biggest existential threat. Retrieved from https://www.theguardian.com/technology/2014/oct/27/elon-musk-artificial-intelligence-ai-biggest-existential-threat

Gibson, C., Maznevski, M., & Kirkman, B. (2009). When does culture matter. *Cambridge handbook of culture, organizations, and work*, 46-70.

Giffin, K. (1967). The contribution of studies of source credibility to a theory of interpersonal trust in the communication process. *Psychological bulletin, 68*(2), 104-120. doi:10.1037/h0024833

Gill, M., & Crane, S. (2017). The role and importance of trust: A study of the conditions that generate and undermine sensitive information sharing. *Security Journal, 30*(3), 734-748.

Gillham, B. (2000). *Research Interview*: Bloomsbury Academic.

Gioia, D. A., & Pitre, E. (1990). Multiparadigm perspectives on theory building. *Academy of management review, 15*(4), 584-602.

Given, L. M. (2008). *The Sage Encyclopedia of Qualitative Research Methods: A-L ; Vol. 2, M-Z Index*: Sage.

Glanz, J., Larson, J., & Lehren, A. W. (2014, January 27). Spy Agencies Tap Data Streaming From Phone Apps. Retrieved from https://www.nytimes.com/2014/01/28/world/spy-agencies-scour-phone-apps-for-personal-data.html

Gleeson, N., & Walden, I. (2014). 'It's a Jungle Out There'?: Cloud Computing, Standards and the Law. *Cloud Computing, Standards and the Law (May 23, 2014)*.

Gliner, J. A., & Morgan, G. A. (2000). *Research methods in applied settings: an integrated approach to design and analysis*: Lawrence Erlbaum.

Gofton, L., & Ness, M. (1997). *Business Market Research*: Kogan Page.

Goldsmith, J. (2018). The failure of internet freedom. *Emerging Threats*.

Golembiewski, R. T., & McConkie, M. (1975). The centrality of interpersonal trust in group processes. *Theories of group processes, 131*, 185.

Good, D. (1988). Individuals, Interpersonal Relations, And Trust. In D. Gambetta (Ed.), *Trust: Making And Breaking Cooperative Relations*. New York: Blackwell.

Goodwin, T. (2015, March 3). The Battle Is For The Customer Interface. Retrieved from https://techcrunch.com/2015/03/03/in-the-age-of-disintermediation-the-battle-is-all-for-the-customer-interface/

Google. (2013a, November 14). Government requests for user information double over three years. Retrieved from https://googleblog.blogspot.com/2013/11/government-requests-for-user.html
Google. (2013b, September 9). A petition for greater transparency. Retrieved from https://googleblog.blogspot.ca/2013/09/petition-for-greater-transparency.html
Google. (2017a). Google Cloud Platform Blog. Retrieved from https://cloudplatform.googleblog.com/
Google. (2017b, May 5). Google Cloud Platform certified to run SAP HANA. Retrieved from https://cloud.google.com/sap/
Gorham-Oscilowski, U., & Jaeger, P. T. (2008). National Security Letters, the USA PATRIOT Act, and the Constitution: The tensions between national security and civil rights. *Government Information Quarterly, 25*(4), 625-644. doi:10.1016/j.giq.2008.02.001
Gounaris, S. P. (2005). Trust and commitment influences on customer retention: insights from business-to-business services. *Journal of Business Research, 58*(2), 126-140.
Goyal, S. (2014). Public vs Private vs Hybrid vs Community-Cloud Computing: A Critical Review. *International Journal of Computer Network and Information Security (IJCNIS), 6*(3), 20-29. doi:10.5815/ijcnis.2014.03.03
Gratton, C., & Jones, I. (2004). *Research Methods for Sport Studies*: Routledge.
Greaver, M. F. (1999). *Strategic Outsourcing: A Structured Approach to Outsourcing Decisions and Initiatives*: AMACOM.
Greene, D. (2016, April 28). First FISC Phone Records Ruling Post-USA FREEDOM Exposes Shortcomings of Reforms. Retrieved from https://www.eff.org/deeplinks/2016/04/first-fisc-phone-records-ruling-post-usa-freedom-exposes-shortcomings-reforms
Greene, J., & Barrett, D. (2016, April 14). Microsoft Sues Justice Department Over Secret Customer Data Searches. Retrieved from http://www.wsj.com/articles/microsoft-sues-justice-department-over-secret-customer-data-searches-1460649720
Greene, R., Kehl, D., Morgus, R., & Bankston, K. (2014). *Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom & Cybersecurity*. Retrieved from
Greener, S. (2008). *Business research methods*: BookBoon.
Greenfield, P. M. (2000). Three approaches to the psychology of culture: Where do they come from? Where can they go? *Asian Journal of Social Psychology, 3*(3), 223-240.
Greenwald, G. (2013a, July 12). Microsoft handed the NSA access to encrypted messages. *The Guardian.* Retrieved from http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data
Greenwald, G. (2013b, June 6). NSA collecting phone records of millions of Verizon customers daily. *The Guardian.* Retrieved from http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order
Greenwald, G. (2013c, July 31). XKeyscore: NSA tool collects 'nearly everything a user does on the internet'. *The Guardian.* Retrieved from http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data
Greis, F. (2014, November 25). Deutsche Nutzer vertrauen der Datensicherheit am wenigsten [German users have the least confidence in data security]. Retrieved from http://www.golem.de/news/nsa-affaere-deutsche-nutzer-vertrauen-der-datensicherheit-am-wenigsten-1411-110778.html
Griffee, D. T. (2005). Research Tips: Interview Data Collection. *Journal of Developmental Education, 28*(3), 36-37.
Griffin, A. (2017, April 4). Donald Trump has signed a law allowing internet companies to sell people's browsing histories. Retrieved from http://www.independent.co.uk/life-style/gadgets-and-tech/news/donald-trump-internet-browsing-history-bill-chrome-federal-communications-commission-a7665821.html

Griffith, D. A., Hu, M. Y., & Jr, J. K. R. (2000). Process Standardization across Intra- and Inter-Cultural Relationships. *Journal of international Business studies, 31*(2), 303-324. doi:10.2307/155639

Guba, E. G. (1990). *The Paradigm Dialog*: SAGE Publications.

Guba, E. G., & Lincoln, Y. S. (1994). Competing paradigms in qualitative research. *Handbook of qualitative research, 2*, 163-194.

Gubrium, J. F., & Holstein, J. A. (2002). *Handbook of interview research : context & method*: Sage Publications.

Guenzi, P., De Luca, L. M., & Spiro, R. (2016). The combined effect of customer perceptions about a salesperson's adaptive selling and selling orientation on customer trust in the salesperson: a contingency perspective. *Journal of Business & Industrial Marketing, 31*(4), 553-564. doi:10.1108/JBIM-02-2015-0037

Guenzi, P., & Georges, L. (2010). Interpersonal trust in commercial relationships: Antecedents and consequences of customer trust in the salesperson. *European Journal of Marketing, 44*(1/2), 114-138. doi:10.1108/03090561011008637

Guest, G., Bunce, A., & Johnson, L. (2006). How many interviews are enough? An experiment with data saturation and variability. *Field methods, 18*(1), 59-82.

Guest, G., MacQueen, K. M., & Namey, E. E. (2011). *Applied Thematic Analysis*: SAGE Publications.

Gueugneau, R. (2012, January 31). Le projet de « cloud computing » à la française irrite IBM. *LesEchos.* Retrieved from http://www.lesechos.fr/31/01/2012/lesechos.fr/0201873061845_le-projet-de---cloud-computing---a-la-francaise-irrite-ibm.htm

Gulati, R., & Sytch, M. (2008). Does Familiarity Breed Trust? Revisiting the Antecedents of Trust. *Managerial and Decision Economics, 29*(2/3), 165-190. doi:10.2307/25151592

Gurun, U. G., Stoffman, N., & Yonker, S. E. (2017). Trust busting: The effect of fraud on investor behavior. *The Review of Financial Studies, 31*(4), 1341-1376.

Gustafsson, V., & Folmerz, M. (2015). The role of trust in business-to-business relationships: The Swedish sales sector.

Gustin, S. (2013, December 10). NSA Spying Scandal Could Cost U.S. Tech Giants Billions. Retrieved from http://business.time.com/2013/12/10/nsa-spying-scandal-could-cost-u-s-tech-giants-billions/

Guynn, J. (2014, January 17). Silicon Valley's reaction to Obama's NSA reforms: Not enough. Retrieved from http://articles.latimes.com/2014/jan/17/business/la-fi-tn-silicon-valleys-reaction-obama-nsa-reforms-20140117

Györy, A. A. B., Cleven, A., Uebernickel, F., & Brenner, W. (2012). *Exploring the shadows: IT governance approaches to user-driven innovation*.

Habib, S. M., Hauke, S., Ries, S., Mühlhäuser, M., Antonopoulos, N., Anjum, A., . . . Rong, C. (2012). Trust as a facilitator in cloud computing: a survey. *Journal of Cloud Computing: Advances, Systems and Applications, 1*(1), 19.

Habib, S. M., Ries, S., & Muhlhauser, M. (2010). *Cloud computing landscape and research challenges regarding trust and reputation.* Paper presented at the Proceedings of the 2010 Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing.

Habib, S. M., Ries, S., Mühlhäuser, M., & Varikkattu, P. (2014). Towards a trust management system for cloud computing marketplaces: using CAIQ as a trust information source. *Security and Communication Networks, 7*(11), 2185-2200.

Hackley, C. (2003). *Doing Research Projects in Marketing, Management and Consumer Research*: Taylor & Francis.

Hackmann, J. (2010, March 15). Brauchen wir eine deutsche Cloud? [Do we need a German cloud?]. Retrieved from http://www.computerwoche.de/a/print/brauchen-wir-eine-deutsche-cloud,1931681

Hackmann, J. (2012, July 25). Ärger um den Patriot Act [Anger about the Patriot Act]. *Computerwoche.* Retrieved from http://www.computerwoche.de/a/aerger-um-den-patriot-act,2503872

Hackmann, J. (2013, June 18). Deutsche Provider zu Prism: Bei uns sind Kundendaten sicher [German providers to Prism: With us, customer data are secure]. *Computerwoche.* Retrieved from http://www.computerwoche.de/a/bei-uns-sind-kundendaten-sicher,2540554

Haffa. (2013, August 1). Business-Cloud-Nutzung nimmt kaum Schaden durch Prism und Tempora [Business cloud use hardly being damaged by Prism and Tempora]. *Dr. Haffa & Partner GmbH.* Retrieved from http://www.haffapartner.de/publicrelations-dr-haffa-partner/aktuelles/01-08-2013-02.html

Haidt, J. (2006). *The happiness hypothesis: Finding modern truth in ancient wisdom*: Basic Books.

Hailén, L., Johanson, J., & Seyed-Mohamed, N. (1991). Interfirm adaptation in business relationships. *Journal of Marketing, 55*(2).

Hall, E. T. (1990). *The Silent Language*: Anchor Books.

Hamlen, K., Kantarcioglu, M., Khan, L., & Thuraisingham, B. (2010). Security issues for cloud computing. *International Journal of Information Security and Privacy (IJISP), 4*(2), 36-48.

Handfield, R. B., & Bechtel, C. (2002). The role of trust and relationship structure in improving supply chain responsiveness. *Industrial Marketing Management, 31*(4), 367-382. doi:10.1016/S0019-8501(01)00169-9

Harding, C. (2011). *Cloud Computing for Business: The Open Group Guide*: Van Haren Publishing.

Harding, J. (2013). *Qualitative Data Analysis from Start to Finish*: SAGE Publications.

Harley, B., Wright, C., Hall, R., & Dery, K. (2006). Management reactions to technological change: The example of enterprise resource planning. *The Journal of Applied Behavioral Science, 42*(1), 58-75.

Harms, R., & Yamartino, M. (2010). The economics of the cloud. *Microsoft.* Retrieved from http://www.microsoft.com/presspass/presskits/cloud/docs/The-Economics-of-the-Cloud.pdf

Harris, A. L., Lang, M., Yates, D., & Kruck, S. E. (2011). Incorporating Ethics and Social Responsibility in IS Education. *Journal of Information Systems Education, 22*(3), 183-189.

Harris Interactive. (1999). *IBM Multinational Consumer Privacy Survey, Study Commissioned by IBM Global Services, October 1999*.

Hasan, H., & Ditsa, G. (1999). The impact of culture on the adoption of IT: An interpretive study. *Journal of Global Information Management (JGIM), 7*(1), 5-15.

Hätönen, J., & Eriksson, T. (2009). 30+ years of research and practice of outsourcing – Exploring the past and anticipating the future. *Journal of International Management, 15*(2), 142-155. doi:10.1016/j.intman.2008.07.002

Hattem, J. (2014, June 30). Tech takes hit from NSA. Retrieved from http://thehill.com/policy/technology/210880-tech-takes-hit-from-nsa

Hawes, J. M., Mast, K. E., & Swan, J. E. (1989). Trust Earning Perceptions of Sellers and Buyers. *The Journal of Personal Selling and Sales Management, 9*(1), 1-8. doi:10.2307/40428338

Hawes, J. M., Rao, C. P., & Baker, T. L. (1993). Retail Salesperson Attributes and the Role of Dependability in the Selection of Durable Goods. *The Journal of Personal Selling and Sales Management, 13*(4), 61-71.

Hawes, J. M., Strong, J. T., & Winick, B. S. (1996). Do closing techniques diminish prospect trust? *Industrial Marketing Management, 25*(5), 349-360.

Hayes, B. (2008). Cloud Computing. *Communications of the ACM, 51*(7), 9-11.

Heidrich, J. (2017, April 13). Auf tönernen Füßen: Warum der Datentransfer in die USA rechtlich riskant ist [On tweaked feet: Why the data transfer to the USA is legally risky]. Retrieved from https://www.heise.de/ct/ausgabe/2017-9-Warum-der-Datentransfer-in-die-USA-rechtlich-riskant-ist-3678248.html

Helmore, E. (2018, Apr 7). What is the Donald Trump v Jeff Bezos feud really about? Retrieved from https://www.theguardian.com/us-news/2018/apr/07/trump-bezos-feud-amazon-washington-post-taxes-usps

Henderson, J. C., & Venkatraman, H. (1999). Strategic alignment: Leveraging information technology for transforming organizations. *IBM systems journal, 38*(2.3), 472-484.

Hennink, M., Hutter, I., & Bailey, A. (2010). *Qualitative Research Methods*: SAGE Publications.

Henze, M., Hiller, J., Hohlfeld, O., & Wehrle, K. (2016). *Moving privacy-sensitive services from public clouds to decentralized private clouds.* Paper presented at the Cloud Engineering Workshop (IC2EW), 2016 IEEE International Conference on.

Hern, A. (2017, Feb 2). Amazon Web Services: the secret to the online retailer's future success. Retrieved from https://www.theguardian.com/technology/2017/feb/02/amazon-web-services-the-secret-to-the-online-retailers-future-success

Hern, A. (2018a, May 25). Facebook and Google targeted as first GDPR complaints filed. Retrieved from https://www.theguardian.com/technology/2018/may/25/facebook-google-gdpr-complaints-eu-consumer-rights

Hern, A. (2018b, 12 Feb). Facebook personal data use and privacy settings ruled illegal by German court. Retrieved from https://www.theguardian.com/technology/2018/feb/12/facebook-personal-data-privacy-settings-ruled-illegal-german-court

Hernandez, J. M. d. C., & dos Santos, C. C. (2010). Development-based Trust: Proposing and Validating a New Trust Measurement Model for Buyer-Seller Relationships. *Brazilian Administration Review, 7*(2), 172-197.

Herrmann, W. (2017, Dec 6). Die besten Cloud-Plattformen im Vergleich [The best cloud platforms in comparison]. Retrieved from https://www.computerwoche.de/a/die-besten-cloud-plattformen-im-vergleich,3332140

Hertzberg, L. (1988). On the attitude of trust. *Inquiry, 31*(3), 307-322.

Heuer, S. (2014). Ist der Ruf erst ruiniert... Was kostet der NSA-Skandal die amerikanische Wirtschaft? Eine Bestandsaufnahme. [Once you've lost your reputation... What does the NSA scandal cost the American economy? An inventory.]. *Brandeins, 10/14 Schwerpunkt Vertrauen*.

Hewett, K., & Bearden, W. O. (2001). Dependence, Trust, and Relational Behavior on the Part of Foreign Subsidiary Marketing Operations: Implications for Managing Global Marketing Operations. *Journal of Marketing, 65*(4), 51-66. doi:10.2307/3203498

Hewett, K., Money, R. B., & Sharma, S. (2002). An exploration of the moderating role of buyer corporate culture in industrial buyer-seller relationships. *Journal of the Academy of Marketing Science, 30*(3), 229-239. doi:10.1177/0092070302303004

Hilary, J. (2015, October 12). I didn't think TTIP could get any scarier, but then I spoke to the EU official in charge of it. Retrieved from http://www.independent.co.uk/voices/i-didn-t-think-ttip-could-get-any-scarier-but-then-i-spoke-to-the-eu-official-in-charge-of-it-a6690591.html

Hill, J. F. (2014). *The growth of data localization post-snowden: Analysis and recommendations for us policymakers and business leaders.* Paper presented at the The Hague Institute for Global Justice, Conference on the Future of Cyber Governance.

Hirsch, F. (1977). *Social Limits to Growth*: Routledge & Kegan Paul.

Hobbes, T. (1650). Human Nature. In D. D. Raphael (1969) (Ed.), *British Moralists, 1650-1800: Hobbes*: Hackett Publishing Company.

Hoberg, P., Wollersheim, J., & Krcmar, H. (2012). *The business perspective on cloud computing-a literature review of research on cloud computing.* Paper presented at the Americas Conference on Information Systems (AMCIS), Seattle, USA.

Hoffmann, W. H., Neumann, K., & Speckbacher, G. (2010). The effect of interorganizational trust on make-or-cooperate decisions: Disentangling opportunism-dependent and opportunism-independent effects of trust. *European Management Review, 7*(2), 101-115.

Hofstede, G. (1991). Cultures and organizations. Intercultural cooperation and its importance for survival. Software of the mind. *London: Mc Iraw-Hill*.

Hofstede, G. (2003a). *Culture's Consequences: Comparing Values, Behaviors, Institutions and Organizations Across Nations*: SAGE Publications.

Hofstede, G. (2003b). What is culture? A reply to Baskerville. *Accounting, Organizations and Society, 28*(7-8), 811-813.

Hofstede, G. (2018, Oct 4). Country Comparison Germany and United States. Retrieved from https://www.hofstede-insights.com/country-comparison/germany,the-usa/

Hofstede, G., & Minkov, M. (2010). Long-versus short-term orientation: new perspectives. *Asia Pacific business review, 16*(4), 493-504.

Holland, S., & Mason, J. (2018, Aug 20). Exclusive: Trump says it is 'dangerous' for Twitter, Facebook to ban accounts. Retrieved from https://www.reuters.com/article/us-usa-trump-tech-exclusive/exclusive-trump-says-dangerous-when-companies-like-twitter-regulate-own-content-idUSKCN1L521D

Hollis, M. (1998). *Trust Within Reason*: Cambridge University Press.

Holtkamp, B. (2010). Cloud Computing für den Mittelstand am Beispiel der Logistikbranche [Cloud computing for small and medium-sized enterprises using the example of the logistics industry]. *Fraunhofer.* Retrieved from http://2011.cebit-studio-mittelstand.de/dlf/0f257de50b0601551cefbbaa604c8c23

Hon, W. K., Millard, C., & Walden, I. (2012). Negotiating cloud contracts: Looking at clouds from both sides now. *Stan. Tech. L. Rev., 16*, 79.

Hoofnagle, C. J., King, J., Li, S., & Turow, J. (2010). How different are young adults from older adults when it comes to information privacy attitudes and policies?

Hosmer, L. T. (1995). Trust: The connecting link between organizational theory and philosophical ethics. *Academy of Management. The Academy of Management Review, 20*(2), 379.

House, R. J., Hanges, P. J., Javidan, M., Dorfman, P. W., & Gupta, V. (2004). *Culture, leadership, and organizations: The GLOBE study of 62 societies*: Sage publications.

Hovenstädt, D. (2013, October 29). Germany's Stasi past looms over NSA spying furor. Retrieved from http://edition.cnn.com/2013/10/29/opinion/nsa-germany-stasi-shadows/

HP. (2011). Finding the right cloud solutions for your organization *Hewlett-Packard Company.* Retrieved from http://h18006.www1.hp.com/storage/pdfs/4AA3-2633ENW.pdf

Huang, J., & Nicol, D. M. (2013). Trust mechanisms for cloud computing. *Journal of Cloud Computing: Advances, Systems and Applications, 2*(1), 9.

Huang, Y., & Wilkinson, I. F. (2013). The dynamics and evolution of trust in business relationships. *Industrial Marketing Management, 42*(3), 455-465.

Huber, G. P., Miller, C. C., & Glick, W. H. (1990). Developing more encompassing theories about organizations: The centralization-effectiveness relationship as an example. *Organization Science, 1*(1), 11-40.

Huerta-Canepa, G., Lee, D., & Han, S. Y. (2011). *Trust me: A trust decision framework for mobile environments.* Paper presented at the 2011IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications.

Huff, L., & Kelley, L. (2003). Levels of Organizational Trust in Individualist versus Collectivist Societies: A Seven-Nation Study, 81.

Hurley, L. (2018, Apr 3). Microsoft calls for dismissal of U.S. Supreme Court privacy fight. Retrieved from https://www.reuters.com/article/us-usa-court-microsoft/microsoft-calls-for-dismissal-of-u-s-supreme-court-privacy-fight-idUSKCN1HA2KH

Husted, B. W. (1989). Trust in business relations: Directions for empirical research. *Business & Professional Ethics Journal*, 23-40.

Huth, S. M. (2004). *Trust in client-service provider relationships.* (PhD), University of Plymouth, Plymouth. Retrieved from http://pearl.plymouth.ac.uk:8080/pearl_xmlui/handle/10026.1/381

Hutt, M. D., & Speh, T. W. (2001). *Business marketing management: A strategic view of industrial and organizational markets*: Thomson/South-Western.

IBM. (2010). Dispelling the vaporaround cloud computing. *International Business Machines Corporation.* Retrieved from ftp://public.dhe.ibm.com/common/ssi/rep_wh/n/CIW03062USEN/CIW03062USEN.PDF

IBM. (2014, January 17). IBM Commits $1.2 Billion to Expand Global Cloud Footprint. Retrieved from http://www-03.ibm.com/press/us/en/pressrelease/42956.wss

IBM. (2015, January 7). IBM Opens First Cloud Data Center With SoftLayer in Germany. Retrieved from http://www-03.ibm.com/press/us/en/pressrelease/45786.wss

IDC. (2012). *IDC-Studie: Cloud Computing in Deutschland 2012 [IDC Study: Cloud Computing in Germany 2012]*. Retrieved from http://www.idc.de/press/presse_idc_studie_cloud2012.jsp

IDC. (2013a). *IDC-Studie: Cloud Computing in Deutschland 2013 [IDC Study: Cloud Computing in Germany 2013]*. Retrieved from

IDC. (2013b). IDC Forecasts Worldwide Public IT Cloud Services Spending to Reach Nearly $108 Billion by 2017 as Focus Shifts from Savings to Innovation [Press release]. Retrieved from http://www.idc.com/getdoc.jsp?containerId=prUS24298013

IDC. (2013c). IDC Predicts 2014 Will Be a Year of Escalation, Consolidation, and Innovation as the Transition to IT's "3rd Platform" Accelerates [Press release]. Retrieved from http://www.idc.com/getdoc.jsp?containerId=prUS24472713

IDC. (2014). *IDC-Studie: Hybrid Clouds werden Realität in deutschen Unternehmen [IDC study: Hybrid Clouds become reality in German companies]*. Retrieved from

IDC. (2015, October 5). IDC Forecasts Worldwide Cloud IT Infrastructure Market to Grow 24% Year Over Year in 2015, Driven by Public Cloud Datacenter Expansion. Retrieved from http://www.idc.com/getdoc.jsp?containerId=prUS25946315

IDC. (2016, January 21). Worldwide Public Cloud Services Spending Forecast to Double by 2019, According to IDC. Retrieved from https://www.idc.com/getdoc.jsp?containerId=prUS40960516

IDC. (2017, January 26). Neue IDC-Studie zeigt: Cloud Disruption in Deutschland in vollem Gang [New IDC study shows: Cloud disruption in Germany in full swing]. Retrieved from http://idc.de/de/ueber-idc/press-center/64573-neue-idc-studie-zeigt-cloud-disruption-in-deutschland-in-vollem-gang

IfM. (2015). Macro-economic significance of SMEs. Retrieved from https://en.ifm-bonn.org/statistics/#accordion=1&tab=0

Inglehart, R. F., Basanez, M., Basanez, M., & Moreno, A. (1998). *Human values and beliefs: A cross-cultural sourcebook*: University of Michigan Press.

Internet Live Stats. (2016, July 1). Internet users in the world. Retrieved from http://www.internetlivestats.com/internet-users

Isabella, L. A. (1990). Evolving Interpretations as a Change Unfolds: How Managers Construe Key Organizational Events. *The Academy of Management Journal, 33*(1), 7-41. doi:10.2307/256350

Ismail, N. (2017, July 18). Trump's presidency could 'cost the US cloud computing industry $10BN'. Retrieved from http://www.information-age.com/trumps-presidency-cost-us-cloud-computing-industry-10bn-123467373/

ITA. (2000). International Trade Administration U.S.-EU Safe Harbor Framework. Retrieved from http://export.gov/safeharbor/eu/index.asp

ITA. (2014). U.S.-EU Safe Harbor List. Retrieved from http://safeharbor.export.gov/list.aspx

Ivanova, I. (2019, Dec 9). Amazon claims Trump pressured Pentagon to give Microsoft cloud computing contract. Retrieved from https://www.cbsnews.com/news/amazon-claims-president-trump-pressured-dod-to-award-microsoft-cloud-computing-contract/

Jabbar, S., Naseer, K., Gohar, M., Rho, S., & Chang, H. (2016). Trust model at service layer of cloud computing for educational institutes. *The Journal of Supercomputing, 72*(1), 58-83.

Jaeger, P. T., Bertot, J. C., & McClure, C. R. (2003). The impact of the USA Patriot Act on collection and analysis of personal information under the Foreign Intelligence Surveillance Act. *Government Information Quarterly, 20*(3), 295-314. doi:10.1016/S0740-624X(03)00057-1

Jaeger, P. T., Lin, J., & Grimes, J. M. (2008). Cloud Computing and Information Policy: Computing in a Policy Cloud? *Journal of Information Technology & Politics, 5*(3), 269-283. doi:10.1080/19331680802425479

Jaiganesh, M., Aarthi, M., & Kumar, A. V. A. (2015). Fuzzy ART-based user behavior trust in cloud computing *Artificial intelligence and evolutionary algorithms in engineering systems* (pp. 341-348): Springer.

James Jr, H. S. (2002). The trust paradox: a survey of economic inquiries into the nature of trust and trustworthiness. *Journal of Economic Behavior & Organization, 47*(3), 291-307. doi:10.1016/S0167-2681(01)00214-1

Jamsa, K. (2012). *Cloud Computing*: Jones & Bartlett Learning.

Jaramillo, F., & Valenzuela, L. (2016). Building Customer Trust and Loyalty: Does Salesperson Empathy Matter? In D. M. Groza & B. C. Ragland (Eds.), *Marketing Challenges in a Turbulent Business Environment: Proceedings of the 2014 Academy of Marketing Science (AMS) World Marketing Congress* (pp. 611-612). Cham: Springer International Publishing.

Jarvenpaa, S. L., Knoll, K., & Leidner, D. E. (1998). Is Anybody out There? Antecedents of Trust in Global Virtual Teams. *Journal of Management Information Systems, 14*(4), 29-64. doi:10.2307/40398291

Jarvenpaa, S. L., & Leidner, D. E. (1998). An information company in Mexico: Extending the resource-based view of the firm to a developing country context. *Information Systems Research, 9*(4), 342-361.

Jarvenpaa, S. L., Tractinsky, N., & Saarinen, L. (1999). Consumer Trust in an Internet Store: A Cross-Cultural Validation. *Journal of Computer-Mediated Communication, 5*(2), 0-0. doi:10.1111/j.1083-6101.1999.tb00337.x

Jayapandian, N., Rahman, A. M. Z., Sangavee, R., & Divya, R. (2016). *Improved cloud security trust on client side data encryption using HASBE and Blowfish.* Paper presented at the 2016 Online International Conference on Green Engineering and Technologies (IC-GET).

Jiang, Z. (2010). *Exploring the Roles of Trust, Reliance and Commitment in Business Relationships.* (Doctoral dissertation), University of Manchester. Retrieved from http://ethos.bl.uk/OrderDetails.do?uin=uk.bl.ethos.511636

Johnson-George, C., & Swap, W. C. (1982). Measurement of specific interpersonal trust: Construction and validation of a scale to assess trust in a specific other. *Journal of Personality and Social Psychology, 43*(6), 1306.

Johnson, D., & Grayson, K. (2005). Cognitive and affective trust in service relationships. *Journal of Business Research, 58*(4), 500-507. doi:10.1016/S0148-2963(03)00140-1

Johnson, J. L., & Cullen, J. B. (2002). Trust in cross-cultural relationships. *The Blackwell Handbook of Cross-Cultural Management*, 335-360.

Johnston, D. A., McCutcheon, D. M., Stuart, F. I., & Kerwood, H. (2004). Effects of supplier trust on performance of cooperative supplier relationships. *Journal of Operations Management, 22*(1), 23-38. doi:10.1016/j.jom.2003.12.001

Jones, D., Behrens, S., Jamieson, K., & Tansley, E. (2004). The rise and fall of a shadow system: Lessons for enterprise system implementation. *ACIS 2004 Proceedings*, 96.

Jones, E., Busch, P., & Dacin, P. (2003). Firm market orientation and salesperson customer orientation: interpersonal and intrapersonal influences on customer service and retention in business-to-business buyer–seller relationships. *Journal of Business Research, 56*(4), 323-340.

Jones, S. (2014, January 31). US spies engaged in industrial espionage will be jailed, says lawmaker. Retrieved from http://www.ft.com/cms/s/0/33001728-8a9b-11e3-ba54-00144feab7de.html

Jones, S., Johnson-Yale, C., Millermaier, S., & Perez, F. S. (2009). Everyday life, online: US college students' use of the Internet. *First Monday, 14*(10).

Jøsang, A. (1996). *The right type of trust for distributed systems.* Paper presented at the Proceedings of the 1996 workshop on New security paradigms.

Julisch, K., & Hall, M. (2010). Security and Control in the Cloud. *Information Security Journal: A Global Perspective, 19*(6), 299-309. doi:10.1080/19393555.2010.514654

Jupp, V. (2006). *The Sage Dictionary of Social Research Methods*: Sage.

Kadidal, S. (2015, December 17). Surveillance After the USA Freedom Act: How Much Has Changed? Retrieved from http://www.huffingtonpost.com/the-center-for-constitutional-rights/surveillance-after-the-us_b_8827952.html

Kâğıtçıbaşı, Ç. (1997). Individualism and collectivism. In J. W. Berry, Y. H. Poortinga, J. Pandey, M. H. Segall, & Ç. Kâğıtçıbaşı (Eds.), *Handbook of Cross-cultural Psychology: Social behavior and applications* (pp. 1-49): Allyn and Bacon.

Kalkman, J. P., & de Waard, E. J. (2017). Inter-organizational disaster management projects: Finding the middle way between trust and control. *International journal of project management, 35*(5), 889-899.

Kant, I. (2005). Groundwork for the Metaphysics of Morals. In L. Denis (Ed.): Broadview Press.

Kanwal, A., Masood, R., Ghazia, U. E., Shibli, M. A., & Abbasi, A. G. (2013, August 20-23). *Assessment Criteria for Trust Models in Cloud Computing.* Paper presented at the Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical and Social Computing.

Kaplan, B., Truex, D. P., Wastell, D., Wood-Harper, A. T., & DeGross, J. I. (2006). *Information Systems Research: Relevant Theory and Informed Practice*: Springer US.

Karnitschnig, M. (2014, February 9). NSA Flap Strains Ties With Europe. Retrieved from http://www.wsj.com/articles/SB10001424052702303874504579372832399168684

Katzan, H., Jr. (2010). On The Privacy Of Cloud Computing. *International Journal of Management and Information Systems, 14*(2), 1-12.

Kaufman, L. M. (2010). Can a trusted environment provide security? *Security & Privacy, IEEE, 8*(1), 50-52.

Kennedy, M. S., Ferrell, L. K., & LeClair, D. T. (2001). Consumers' trust of salesperson and manufacturer: an empirical study. *Journal of Business Research, 51*(1), 73-86. doi:10.1016/S0148-2963(99)00039-9

Kenneth, C. (2012, January 19). Foreign Cloud Privacy Issues Dismissed by U.S. Officials. Retrieved from http://www.cio.com/article/698312/Foreign_Cloud_Privacy_Issues_Dismissed_by_U.S._Officials

Kerkmann, C. (2013a, June 13). US-Schnüffelei: Schwarze Wolken [US snooping: Black clouds]. *Handelsblatt.* Retrieved from http://www.handelsblatt.com/unternehmen/it-medien/us-schnueffelei-im-internet-schwarze-wolken/8337950.html

Kerkmann, C. (2013b, February 21). Viele Firmen fürchten die Datenwolke [Many companies fear the Cloud]. Retrieved from http://www.handelsblatt.com/technologie/it-tk/cebit-special-2013/trends/cebit-leitthema-viele-firmen-fuerchten-die-datenwolke-seite-all/7818826-all.html

Kerr, J., & Teng, K. (2012). Cloud computing: legal and privacy issues. *Journal of Legal Issues and Cases in Business, 1*, 1-11.

Kerr, O. (2003). Internet surveillance law after the USA Patriot Act: The big brother that isn't. *Northwestern University Law Review, 97*.

Kesan, J. P., Hayes, C. M., & Bashir, M. N. (2013). Information Privacy and Data Control in Cloud Computing: Consumers, Privacy Preferences, and Market Efficiency. *Washington and Lee Law Review, 70*(1), 341-472.

Khajeh-Hosseini, A., Sommerville, I., & Sriram, I. (2010). Research challenges for enterprise cloud computing. *arXiv preprint arXiv:1001.3257*.

Khan, K. M., & Malluhi, Q. (2010). Establishing trust in cloud computing. *IEEE Computer Society IT professional, 12*(5), 20-27.

Khan, K. M., & Malluhi, Q. M. (2013). Trust in Cloud Services: Providing More Controls to Clients. *IEEE Computer, 46*(7), 94-96.

Khorshed, M. T., Ali, A. S., & Wasimi, S. A. (2012). A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. *Future Generation computer systems, 28*(6), 833-851.

Killam, L. (2013). *Research terminology simplified: Paradigms, axiology, ontology, epistemology and methodology*: Laura Killam.

Kim, P. H., Ferrin, D. L., Cooper, C. D., & Dirks, K. T. (2004). Removing the shadow of suspicion: the effects of apology versus denial for repairing competence-versus integrity-based trust violations. *Journal of Applied Psychology, 89*(1), 104.

King, N. (2004). Using templates in the thematic analysis of text. *Essential guide to qualitative methods in organizational research, 2*, 256-270.

King, N., & Horrocks, C. (2010). *Interviews in Qualitative Research*: SAGE Publications.

King, R. (2014, January 8). NSA Fears Prompt Companies to Move Data Out of U.S. Retrieved from http://blogs.wsj.com/cio/2014/01/08/nsa-fears-prompt-companies-to-move-data-out-of-u-s/

Kirschbaum, E. (2014, January 26). Snowden says NSA engages in industrial espionage: TV. Retrieved from http://www.reuters.com/article/us-security-snowden-germany-idUSBREA0P0DE20140126

Kishore, R., Rao, H. R., Nam, K., Rajagopalan, S., & Chaudhury, A. (2003). A relationship perspective on IT outsourcing. *Communications of the ACM, 46,* 86-92.

Klandermans, B., & Staggenborg, S. (2002). *Methods of Social Movement Research*: University of Minnesota Press.

Klenke, K. (2008). *Qualitative research in the study of leadership*: Emerald.

Kluckhohn, F. R., & Strodtbeck, F. L. (1961). Variations in value orientations.

Knight, W. (2017, April 11). The Dark Secret at the Heart of AI. Retrieved from https://www.technologyreview.com/s/604087/the-dark-secret-at-the-heart-of-ai/

Ko, R. K., Jagadpramana, P., Mowbray, M., Pearson, S., Kirchberg, M., Liang, Q., & Lee, B. S. (2011). *TrustCloud: A framework for accountability and trust in cloud computing.* Paper presented at the 2011 IEEE World Congress on Services.

Koh, T. K., Fichman, M., & Kraut, R. E. (2012). Trust across borders: Buyer-supplier trust in global Business-to-Business e-commerce.

Koh, T. K., Fichman, M., & Kraut, R. E. (2012). Trust Across Borders: Buyer-Supplier Trust in Global Business-to-Business E-Commerce. *Journal of the Association for Information Systems, 13*(11), 886-922.

Kolb, B. (2008). *Marketing Research: A Practical Approach*: SAGE.
König, N., & Schuknecht, L. (2018). The Role of Government and Trust in the Market Economy.
KPMG. (2012). *Modeling the Economic Impact of Cloud Computing*. Retrieved from https://www.kpmg.com/AU/en/IssuesAndInsights/ArticlesPublications/Documents/modelling-economic-impact-cloud-computing.pdf
KPMG. (2013). *The cloud takes shape* Retrieved from http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/cloud-service-providers-survey/Documents/the-cloud-takes-shape-v4.pdf
KPMG. (2014). *Cloud Monitor 2014*: KPMG AG Wirtschaftsprüfungsgesellschaft.
KPMG. (2015). *Cloud Monitor 2015*: KPMG AG Wirtschaftsprüfungsgesellschaft.
KPMG. (2016). *Cloud Monitor 2016*: KPMG AG Wirtschaftsprüfungsgesellschaft.
KPMG. (2017a). *Cloud Monitor 2017*: KPMG AG Wirtschaftsprüfungsgesellschaft.
KPMG. (2017b, March 17). Cloud Monitor 2017: Die Wolke hat sich etabliert [The cloud has established itself]. Retrieved from https://home.kpmg.com/de/de/home/themen/2017/03/cloud-monitor-2017-vorbestellung.html
Krasnova, H., & Veltri, N. F. (2010). *Privacy calculus on social networking sites: Explorative evidence from Germany and USA.* Paper presented at the System sciences (HICSS), 2010 43rd Hawaii international conference on.
Krasnova, H., & Veltri, N. F. (2011). *Behind the curtains of privacy calculus on social networking sites: the study of Germany and the USA*.
Krasnova, H., Veltri, N. F., & Günther, O. (2012). Self-disclosure and privacy calculus on social networking sites: The role of culture. *Business & Information Systems Engineering, 4*(3), 127-135.
Kravets, D. (2017, Jun 24). Does US have right to data on overseas servers? We're about to find out. Retrieved from https://arstechnica.com/tech-policy/2017/06/supreme-court-asked-to-decide-if-us-has-right-to-data-on-foreign-servers/
Krishnan, R., Martin, X., & Noorderhaven, N. G. (2006). When Does Trust Matter to Alliance Performance? *The Academy of Management Journal, 49*(5), 894-917. doi:10.2307/20159808
Kroeber, A. L., & Kluckhohn, C. (1952). Culture: A critical review of concepts and definitions. *Papers. Peabody Museum of Archaeology & Ethnology, Harvard University*.
Kshetri, N. (2013). Privacy and security issues in cloud computing: The role of institutions and institutional evolution. *Telecommunications Policy, 37*(4-5), 372-386.
Kumar, N., Scheer, L. K., & Steenkamp, J.-B. E. M. (1995). The effects of perceived interdependence on dealer attitudes. *JMR, Journal of Marketing Research, 32*(3), 348.
Kushida, K., Murray, J., & Zysman, J. (2011). Diffusing the Cloud: Cloud Computing and Implications for Public Policy. *Journal of Industry, Competition and Trade, 11*(3), 209-237. doi:10.1007/s10842-011-0106-5
Kushida, K., Murray, J., & Zysman, J. (2012). The Gathering Storm: Analyzing the Cloud Computing Ecosystem and Implications for Public Policy. *Communications & Strategies*(85), 63-85,220-221,223.
Kvale, S. (1996). *Interviews: an introduction to qualitative research interviewing*: Sage Publications.
Kwon, I.-W. G., & Suh, T. (2004). Factors Affecting the Level of Trust and Commitment in Supply Chain Relationships. *Journal of Supply Chain Management, 40*(1), 4-14. doi:10.1111/j.1745-493X.2004.tb00165.x
Kwon, I.-W. G., & Suh, T. (2005). Trust, commitment and relationships in supply chain management: a path analysis. *Supply chain management: an international journal, 10*(1), 26-33.

Lagace, R. R., Dahlstrom, R., & Gassenheimer, J. B. (1991). The Relevance of Ethical Salesperson Behavior on Relationship Quality: The Pharmaceutical Industry. *The Journal of Personal Selling and Sales Management, 11*(4), 39-47. doi:10.2307/20832471

Lagerspetz, O. (1998). *Trust: The Tacit Demand*: Springer.

Lahno, B. (1999). Olli Lagerspetz: Trust. The Tacit Demand. *Ethical Theory and Moral Practice, 2*(4), 433-435. doi:10.1023/A:1009935315332

Lamarque, K. (2014, January 17). U.S.-Germany relations hit new low amid NSA spying scandal, official says. Retrieved from http://worldnews.nbcnews.com/_news/2014/01/17/22338261-us-germany-relations-hit-new-low-amid-nsa-spying-scandal-official-says

Lanois, P. (2010). Caught in the Clouds: The Web 2.0, Cloud Computing, and Privacy? *Northwestern Journal of Technology and Intellectual Property, 9*(2), 29.

Lansing, J., & Sunyaev, A. (2016). Trust in Cloud Computing: Conceptual Typology and Trust-Building Antecedents. *SIGMIS Database, 47*(2), 58-96. doi:10.1145/2963175.2963179

Lapadat, J. C., & Lindsay, A. C. (1999). Transcription in research and practice: From standardization of technique to interpretive positionings. *Qualitative inquiry, 5*(1), 64-86.

Lapowsky, I. (2018, Dec 11). THE SUNDAR PICHAI HEARING WAS A MAJOR MISSED OPPORTUNITY. Retrieved from https://www.wired.com/story/congress-sundar-pichai-google-ceo-hearing/

Larzelere, R. E., & Huston, T. L. (1980). The dyadic trust scale: Toward understanding interpersonal trust in close relationships. *Journal of Marriage and the Family*, 595-604.

Latif, R., Abbas, H., Assar, S., & Ali, Q. (2014). Cloud computing risk assessment: a systematic literature review *Future information technology* (pp. 285-295): Springer.

Lauchlan, S. (2016, April 14). US cloud providers take note – Europe's new data regime begins in 2018. Retrieved from http://diginomica.com/2016/04/14/us-cloud-providers-take-note-europes-new-data-regime-begins-in-2018/

Layard, R. (2011). *Happiness: Lessons from a new science*: Penguin UK.

Lee, C. (2016, Dec 2). Too many UK politicians are clueless about tech. Retrieved from https://www.techworld.com/security/too-many-uk-politicians-are-clueless-about-tech-3625100/

Lee, D. Y., & Dawes, P. L. (2005). Guanxi, Trust, and Long-Term Orientation in Chinese Business Markets. *Journal of International Marketing, 13*(2), 28-56. doi:10.2307/25049008

Lee, J.-N., & Choi, B. (2011). Effects of initial and ongoing trust in IT outsourcing: A bilateral perspective. *Information & Management, 48*(2–3), 96-105. doi:10.1016/j.im.2011.02.001

Lee, J.-N., Huynh, M. Q., & Hirschheim, R. (2008). An integrative model of trust on IT outsourcing: Examining a bilateral perspective. *Information Systems Frontiers, 10*(2), 145-163. doi:10.1007/s10796-008-9066-7

Lee, M. K., & Turban, E. (2001). A trust model for consumer internet shopping. *International Journal of Electronic Commerce, 6*(1), 75-91.

Leidner, D. E., & Kayworth, T. (2006). A review of culture in information systems research: Toward a theory of information technology culture conflict. *Mis Quarterly, 30*(2), 357-399.

Leimeister, S., Böhm, M., Riedl, C., & Krcmar, H. (2010). *The business perspective of cloud computing: Actors, roles and value networks.* Paper presented at the 18th European Conference on Information Systems (ECIS 2010), Pretoria, South Africa.

Lenhart, A., & Madden, M. (2007a). Social networking websites and teens: An overview.

Lenhart, A., & Madden, M. (2007b). Teens, privacy, and online social networks. Pew Internet & American Life Project report.
Leung, T., Lai, K.-h., Chan, R. Y., & Wong, Y. (2005). The roles of "xinyong" and "guanxi" in Chinese relationship marketing. *European Journal of Marketing, 39*(5/6), 528-559.
Levy, S. (2014, January 7). How the NSA almost killed the Internet. Retrieved from https://www.wired.com/2014/01/how-the-us-almost-killed-the-internet/
Lewan, M. (2018). The role of trust in emerging technologies *The Rise and Development of FinTech* (pp. 111-129): Routledge.
Lewicki, R. J., & Bunker, B. B. (1996). Developing and maintaining trust in work relationships. *Trust in organizations: Frontiers of theory and research, 114*, 139.
Lewis-Beck, M. S., Bryman, A., & Liao, T. F. (2004). *The Sage encyclopedia of social science research methods*: Sage.
Lewis, J. D. (2007). *Trusted Partners: How Companies Build Mutual Trust and Win Together*: Free Press.
Lewis, J. D., & Weigert, A. (1985a). Social Atomism, Holism, and Trust. *The Sociological Quarterly, 26*(4), 455-471. doi:10.2307/4106098
Lewis, J. D., & Weigert, A. (1985b). Trust as a Social Reality. *Social Forces, 63*(4), 967-985. doi:10.2307/2578601
Li, J., Li, J., Chen, X., Jia, C., & Lou, W. (2015). Identity-based encryption with outsourced revocation in cloud computing. *Ieee Transactions on computers, 64*(2), 425-437.
Lichter, A., Löffler, M., & Siegloch, S. (2016). The Long-Term Costs of Government Surveillance: Insights from Stasi Spying in East Germany.
Lifen Zhao, A., Koenig-Lewis, N., Hanmer-Lloyd, S., & Ward, P. (2010). Adoption of internet banking services in China: is it all about trust? *International Journal of Bank Marketing, 28*(1), 7-26.
Lim, K. H., Leung, K., Sia, C. L., & Lee, M. K. (2004). Is eCommerce boundary-less? Effects of individualism–collectivism and uncertainty avoidance on Internet shopping. *Journal of international Business studies, 35*(6), 545-559.
Lind, E. A., & Earley, P. C. (1992). Procedural justice and culture. *International Journal of Psychology, 27*(2), 227-242.
Lindskold, S. (1978). Trust development, the GRIT proposal, and the effects of conciliatory acts on conflict and cooperation. *Psychological bulletin, 85*(4), 772.
Lindskold, S., & Bennett, R. (1973). Attributing trust and conciliatory intent from coercive power capability. *Journal of Personality and Social Psychology, 28*(2), 180.
Linthicum, D. (2012, January 24). The E.U.'s cynical campaign against U.S. cloud providers. Retrieved from http://www.infoworld.com/d/cloud-computing/the-eus-cynical-campaign-against-us-cloud-providers-184748
Linthicum, D. (2013, June 11). Thanks, NSA, you're killing the cloud. *InfoWorld.* Retrieved from http://www.infoworld.com/d/cloud-computing/thanks-nsa-youre-killing-the-cloud-220434
Liu, A. H., & Leach, M. P. (2001). Developing loyal customers with a value-adding sales force: Examining customer satisfaction and the perceived credibility of consultative salespeople. *Journal of Personal Selling & Sales Management, 21*(2), 147-156.
Liu, E. C. (2011). Amendments to the Foreign Intelligence Surveillance Act (FISA) Extended Until June 1, 2015 *Congressional Research Service Report Prepared for Members and Committees of Congress.* Retrieved from http://www.fas.org/sgp/crs/intel/R40138.pdf
Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., & Leaf, D. (2011). NIST Cloud Computing Reference Architecture. *National Institute of Standards and Technology.* Retrieved from http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505
Liu, Y.-C., Ma, Y.-T., Zhang, H.-S., Li, D.-Y., & Chen, G.-S. (2011). A method for trust management in cloud computing: Data coloring by cloud watermarking. *International journal of automation and computing, 8*(3), 280.

Lonsdale, C., & Cox, A. (2000). The historical development of outsourcing: the latest fad? *Industrial management & data systems, 100*(9), 444-450.
Lorenz, E. (1988). Neither Friends nor Strangers: Informal Networks of Subcontracting in French Industry. In D. Gambetta (Ed.), *Trust: Making and Breaking Cooperative Relations* (pp. 194-210). Department of Sociology: University of Oxford.
Lorenz, E. (1999). Trust, contract and economic cooperation. *Cambridge journal of economics, 23*(3), 301-315.
Low, C., Chen, Y., & Wu, M. (2011). Understanding the determinants of cloud computing adoption. *Industrial management & data systems, 111*(7), 1006-1023.
Luftman, J., & Kempaiah, R. (2007). An update on business-IT alignment:“A line” has been drawn. *MIS Quarterly Executive, 6*(3), 165-177.
Luhmann, N., Davis, H., Raffan, J., & Rooney, K. (1979). *Trust and power: two works by Niklas Luhmann*: Wiley Chichester.
Lukenbill, G. (1999). Consumers Most Worried About Privacy, Polls Find. *DM News*.
Luo, Y. (2000). *Multinational Corporations in China: Benefiting from Structural Transformation*: Copenhagen Business School Press.
Lynn, T., Van Der Werff, L., Hunt, G., & Healy, P. (2016). Development of a cloud trust label: a Delphi approach. *Journal of Computer Information Systems, 56*(3), 185-193.
MacAskill, E., Borger, J., Hopkins, N., Davies, N., & Ball, J. (2013, June 21). GCHQ taps fibre-optic cables for secret access to world's communications. *The Guardian.* Retrieved from http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa
Machin, S., & Van Reenen, J. (1998). Technology and changes in skill structure: evidence from seven OECD countries. *The Quarterly journal of economics, 113*(4), 1215-1244.
Macías, M., & Guitart, J. (2016). Analysis of a trust model for SLA negotiation and enforcement in cloud markets. *Future Generation computer systems, 55*, 460-472. doi:10.1016/j.future.2015.03.011
Madhok, A. (1995). Revisiting multinational firms' tolerance for joint ventures: a trust-based approach. *Journal of international Business studies*, 117-137.
Mahajan, A., Bishop, J. W., & Scott, D. (2012). Does trust in top management mediate top management communication, employee involvement and organizational commitment relationships? *Journal of Managerial Issues*, 173-190.
Maister, D. H., Green, C. H., & Galford, R. M. (2000). *The trusted advisor*: Simon and Schuster.
Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research, 15*(4), 336-355.
Manta, C. (2011, November 15). Aufs Wesentliche konzentrieren [Focus on the essentials]. *Computerwoche.* Retrieved from http://www.computerwoche.de/a/aufs-wesentliche-konzentrieren,2498596
Manuel, P. (2015). A trust model of cloud computing based on Quality of Service. *Annals of Operations Research, 233*(1), 281-292. doi:10.1007/s10479-013-1380-x
Marinescu, D. C. (2017). *Cloud Computing: Theory and Practice*: Elsevier Science.
Marnau, N., & Schlehahn, E. (2011). Cloud Computing und Safe Harbor. *Datenschutz und Datensicherheit - DuD, 35*(5), 311-316. doi:10.1007/s11623-011-0077-z
Marschan-Piekkari, R., & Welch, C. (2004). *Handbook of qualitative research methods for international business*: Edward Elgar.
Marshall, C., & Rossman, G. B. (2010). *Designing Qualitative Research*: Sage.
Marshall, M. N. (1996). The key informant technique. *Family practice, 13*(1), 92-97.
Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing—The business perspective. *Decision Support Systems, 51*(1), 176-189.
Martens, B., & Teuteberg, F. (2012). Decision-making in cloud computing environments: A cost and risk based approach. *Information Systems Frontiers, 14*(4), 871-893.

Martucci, L. A., Zuccato, A., Smeets, B., Habib, S. M., Johansson, T., & Shahmehri, N. (2012, 4-7 Sept. 2012). *Privacy, Security and Trust in Cloud Computing: The Perspective of the Telecommunication Industry.* Paper presented at the Ubiquitous Intelligence & Computing and 9th International Conference on Autonomic & Trusted Computing (UIC/ATC), 2012 9th International Conference on.

Marwick, A. E., Murgia-Diaz, D., & Palfrey, J. G. (2010). Youth, privacy and reputation (literature review).

Mascolo, G., & Scott, B. (2013). Lessons from the Summer of Snowden: The Hard Road Back to Trust. Retrieved from https://www.wilsoncenter.org/sites/default/files/NAF-OTI-WC-SummerOfSnowdenPaper.pdf

Maslow, A. H. (1943). A theory of human motivation. *Psychological review, 50*(4), 370.

Mason, J. (2002). *Qualitative researching*: Sage Publications.

Mastro, V. A., & Wells, A. (2014). *The Boy Who Cried Wolf: An Aesop's fable from Aesop's Childhood Adventures*: BookBaby.

Mauerer, J. (2016, March 23). Pragmatismus verdrängt die Cloud-Angst [Pragmatism displaces the fear of the cloud]. Retrieved from http://www.computerwoche.de/a/print/pragmatismus-verdraengt-die-cloud-angst,3225234

Maxwell, J. A. (2005). *Qualitative research design: an interactive approach*: Sage Publications.

Maxwell, W., & Wolf, C. (2012, July 18). A Global Reality: Governmental Access to Data in the Cloud. *A Hogan Lovells White Paper.* Retrieved from http://www.hldataprotection.com/uploads/file/Revised%20Government%20Access%20to%20Cloud%20Data%20Paper%20(18%20July%2012).pdf

Maxwell, W., & Wolf, C. (2013, May 22). A Sober Look at National Security Access to Data in the Cloud. *A Hogan Lovells White Paper.* Retrieved from http://www.hldataprotection.com/files/2013/05/A-Sober-Look-at-National-Security-Access-to-Data-in-the-Cloud.pdf

Mayeda, A. (2018, Dec 14). $1 Billion a Month: The Cost of Trump's Tariffs on Technology. Retrieved from https://www.bloomberg.com/news/articles/2018-12-14/-1-billion-a-month-the-cost-of-trump-s-tariffs-on-technology

Mayer, M., & Bell, R. (2013, June 17). Our Commitment to Our Users' Privacy. Retrieved from https://yahoo.tumblr.com/post/53243441454/our-commitment-to-our-users-privacy

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integration model of organizational trust. *Academy of Management. The Academy of Management Review, 20*(3), 709.

Maynard, M. L., & Taylor, C. R. (1996). A comparative analysis of Japanese and US attitudes toward direct marketing. *Journal of Direct Marketing, 10*(1), 34-44.

McAllister, D. J. (1995). Affect- and cognition-based trust as foundations for interpersonal cooperations in organizations. *Academy of Management Journal, 38*(1), 24.

McCole, P., Ramsey, E., & Williams, J. (2010). Trust considerations on attitudes towards online purchasing: The moderating effect of privacy and security concerns. *Journal of Business Research, 63*(9-10), 1018-1024.

McCullagh, D. (2013, June 14). Facebook, Microsoft release NSA stats to reassure users. Retrieved from http://www.cnet.com/news/facebook-microsoft-release-nsa-stats-to-reassure-users/

McKendrick, J. (2012, March 5). NIST definition of cloud computing doesn't go far enough [Web log post]. *ZDNet*. Retrieved from http://www.zdnet.com/blog/service-oriented/nist-definition-of-cloud-computing-doesnt-go-far-enough/8634

McKernan, J., & James, M. K. (2013). *Curriculum Action Research: A Handbook of Methods and Resources for the Reflective Practitioner*: Taylor & Francis.

McKinsey. (2016, September 17). IT as a service: From build to consume. Retrieved from http://www.mckinsey.com/industries/high-tech/our-insights/it-as-a-service-from-build-to-consume

McKnight, D. H., & Chervany, N. L. (2001). What Trust Means in E-Commerce Customer Relationships: An Interdisciplinary Conceptual Typology. *International Journal of Electronic Commerce, 6*(2), 25.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research, 13*(3), 334-359.

McKnight, D. H., Cummings, L. L., & Chervany, N. L. (1998). Initial trust formation in new organizational relationships. *Academy of management review, 23*(3), 473-490.

Meisner, J. (2013, December 8). Reforming government surveillance. Retrieved from https://blogs.technet.microsoft.com/microsoft_on_the_issues/2013/12/08/reforming-government-surveillance/

Meisner, J. (2014, March 26). Microsoft becomes the first global public cloud provider in China with the general availability of Microsoft Azure in the region. Retrieved from https://blogs.technet.microsoft.com/microsoft_blog/2014/03/26/microsoft-becomes-the-first-global-public-cloud-provider-in-china-with-the-general-availability-of-microsoft-azure-in-the-region/

Mellinger, G. D. (1956). Interpersonal trust as a factor in communication. *The Journal of Abnormal and Social Psychology, 52*(3), 304.

Menguc, B., Auh, S., & Kim, Y. C. (2011). Salespeople's knowledge-sharing behaviors with coworkers outside the sales unit. *Journal of Personal Selling & Sales Management, 31*(2), 103-122.

Menn, J. (2013, Decembe 20). Exclusive: Secret contract tied NSA and security industry pioneer. *Reuters.* Retrieved from http://www.reuters.com/article/2013/12/20/us-usa-security-rsa-idUSBRE9BJ1C220131220

Merriam, S. B. (2014). *Qualitative Research: A Guide to Design and Implementation*: Wiley.

Mertens, D. M. (2014). *Research and Evaluation in Education and Psychology: Integrating Diversity With Quantitative, Qualitative, and Mixed Methods*: SAGE Publications.

Messmer, E. (2013, July 19). U.S. high-tech industry feeling the heat from Edward Snowden leaks. Retrieved from http://www.networkworld.com/article/2168328/security/u-s--high-tech-industry-feeling-the-heat-from-edward-snowden-leaks.html

Metz, C. (2016, September 25). Microsoft Bets Its Future on a Reprogrammable Computer Chip. Retrieved from https://www.wired.com/2016/09/microsoft-bets-future-chip-reprogram-fly/

Meyer, J.-B. (2013, September 19). Cloud in Zeiten von Prism: Interview mit Hagen Rickmann, T-Systems [Cloud in Times of Prism: Interview with Hagen Rickmann, T-Systems]. *CIO.* Retrieved from http://www.cio.de/was_ist_cloud_computing/anbieter/2930824/index.html

MGI. (2013). *Disruptive technologies: Advances that will transform life, business, and the global economy* Retrieved from http://www.mckinsey.com/~/media/McKinsey/dotcom/Insights%20and%20pubs/MGI/Research/Technology%20and%20Innovation/Disruptive%20technologies/MGI_Disruptive_technologies_Executive_summary_May2013.ashx

Michael, B. (2009). In Clouds Shall We Trust? *IEEE Security & Privacy, 7*, 3-3.

Microsoft. (2010). Datacenter Management and Virtualization. *Microsoft Corporation.* Retrieved from http://download.microsoft.com/download/7/7/A/77A7BB13-5A36-4924-864E-7EA740F42E4F/Datacenter-Management-and-Virtualization_white-paper.pdf

Microsoft. (2013). *Small and midsize businesses cloud trust study: Germany study results*. Retrieved from

https://news.microsoft.com/download/presskits/security/docs/TwCJune13Germany.pdf
Microsoft. (2015, November 11). Microsoft Announces Plans to Offer Cloud Services from German Datacenters. Retrieved from https://news.microsoft.com/europe/2015/11/11/45283/
Microsoft. (2016, August 10). Azure Information Protection with HYOK (Hold Your Own Key). Retrieved from https://blogs.technet.microsoft.com/enterprisemobility/2016/08/10/azure-information-protection-with-hyok-hold-your-own-key/
Microsoft. (2017a). Microsoft Azure Blog. Retrieved from https://azure.microsoft.com/en-us/blog/
Microsoft. (2017b, May 5). SAP on Azure. Retrieved from https://azure.microsoft.com/en-us/solutions/sap/
Microsoft. (2018, May 25). Preparing for a new era in privacy regulation. Retrieved from https://www.microsoft.com/en-us/TrustCenter/Privacy/gdpr/default.aspx
Milberg, S. J., Smith, H. J., & Burke, S. J. (2000). Information privacy: Corporate management and national regulation. *Organization Science, 11*(1), 35-57.
Millard, C. (2013). *Cloud Computing Law*: OUP Oxford.
Miller, C. C. (2014, March 21). Revelations of N.S.A. Spying Cost U.S. Tech Companies. Retrieved from http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html
Miloslavskaya, N., & Tolstoy, A. (2016). Big data, fast data and data lake concepts. *Procedia Computer Science, 88*, 300-305.
Miltgen, C. L., & Peyrat-Guillard, D. (2014). Cultural and generational influences on privacy concerns: a qualitative study in seven European countries. *European Journal of Information Systems, 23*(2), 103-125.
Mintzberg, H. (1978). Patterns in strategy formation. *Management science, 24*(9), 934-948.
Mir, R., & Watson, A. (2000). Strategic management and the philosophy of science: The case for a constructivist methodology. *Strategic Management Journal*, 941-953.
Mirobi, G. J., & Arockiam, L. (2015). *Service level agreement in cloud computing: an overview.* Paper presented at the 2015 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT).
Misztal, B. (2013). *Trust in Modern Societies: The Search for the Bases of Social Order*: Wiley.
Molinsky, A. (2007). Cross-cultural code-switching: The psychological challenges of adapting behavior in foreign cultural interactions. *Academy of management review, 32*(2), 622-640.
Möllering, G. (2002). Perceived trustworthiness and inter-firm governance: empirical evidence from the UK printing industry. *Cambridge journal of economics, 26*(2), 139-160.
Monsen, E. R., & Van Horn, L. (2007). *Research: Successful Approaches*: American Dietetic Association.
Moody, G. (2015, November 12). Microsoft building data centers in Germany that US government can't touch. Retrieved from http://arstechnica.com/information-technology/2015/11/microsoft-is-building-data-centres-in-germany-that-the-us-government-cant-touch/
Moorman, C., Deshpande, R., & Zaltman, G. (1993). Factors affecting trust in market research relationships. *Journal of Marketing, 57*(1), 81.
Moorman, C., Zaltman, G., & Deshpande, R. (1992). Relationships Between Providers and Users of Market Research: The Dynamics of Trust Within and Between Organizations. *JMR, Journal of Marketing Research, 29*(3), 314.
Morgan, R. M. (1991). *Relationship commitment and trust in marketing.* (Ph.D.), Texas Tech University.

Morgan, R. M., & Hunt, S. D. (1994). The commitment-trust theory of relationship marketing. *Journal of Marketing, 58*(3), 20.

Mortsiefer, H. (2013, July 3). Wirtschaft stellt das Freihandelsabkommen in Frage [Economy questioned the free trade agreement]. Retrieved from http://www.tagesspiegel.de/wirtschaft/snowden-und-die-us-spionage-wirtschaft-stellt-das-freihandelsabkommen-in-frage/8438602.html

Moscardelli, D. M., & Divine, R. (2007). Adolescents' concern for privacy when using the Internet: An empirical analysis of predictors and relationships with privacy-protecting behaviors. *Family and Consumer Sciences Research Journal, 35*(3), 232-252.

Moscardelli, D. M., & Liston-Heyes, C. (2004). Teens surfing the net: How do they learn to protect their privacy. *Journal of Business and Economics Research, 2*(9), 43-56.

Mualla, K., & Jenkins, D. (2015). Evaluating cloud computing challenges for non-expert decision-makers. *International Journal of Digital Information and Wireless Communications, 5*(4), 285-297.

Muchahari, M. K., & Sinha, S. K. (2012, December 17-18). *A New Trust Management Architecture for Cloud Computing Environment.* Paper presented at the Cloud and Services Computing (ISCOS), 2012 International Symposium on.

Müller, D., & Witmer-Goßner, E. (2015, April 15). German Angst in der IT. Retrieved from http://www.cloudcomputing-insider.de/german-angst-in-der-it-a-485909/

Mureșan, R. (2016). The emotional side of virtualization: how trust affects cloud adoption and security decisions. Retrieved from https://download.bitdefender.com/resources/files/News/CaseStudies/study/147/Bitdefender-Business-2017-Whitepaper-Hybrids-c1074-en-EN-web.pdf

Murphy, J. T. (2006). Building trust in economic space. *Progress in Human Geography, 30*(4), 427-450.

Murray, T. (2017, March 31). While Trump Tries To Throw The U.S. Climate Agenda Into Reverse, Leading Businesses Speed Forward. Retrieved from https://www.forbes.com/sites/edfenergyexchange/2017/03/31/while-trump-tries-to-throw-the-u-s-climate-agenda-into-reverse-leading-businesses-speed-forward/#5a38a5af34ab

Myers, M. D., & Tan, F. B. (2003). Beyond models of national culture in information systems research. In B. T. Felix (Ed.), *Advanced topics in global information management* (pp. 14-29): IGI Global.

Nakashima, E. (2015, March 24). Tech firms and privacy groups press for curbs on NSA surveillance powers. Retrieved from http://www.washingtonpost.com/world/national-security/tech-firms-and-privacy-groups-press-for-curbs-on-nsa-surveillance-powers/2015/03/24/4d35772c-d249-11e4-ab77-9646eea6a4c7_story.html

Nakashima, E. (2016, October 14). Justice Dept. asks court to review decision on Microsoft emails held in Ireland. Retrieved from https://www.washingtonpost.com/world/national-security/justice-department-appeals-court-decision-on-access-to-microsoft-emails-held-in-ireland/2016/10/14/1a1ac910-920e-11e6-a6a3-d50061aa9fae_story.html

Nakashima, E. (2018, Mar 31). Justice Department asks Supreme Court to moot Microsoft email case, citing new law. Retrieved from https://www.washingtonpost.com/world/national-security/justice-department-asks-supreme-court-to-moot-microsoft-email-case-citing-new-law

Nakayachi, K., & Watabe, M. (2005). Restoring trustworthiness after adverse events: The signaling effects of voluntary “hostage posting” on trust. *Organizational behavior and human decision processes, 97*(1), 1-17.

Nardon, L., & Steers, R. M. (2009). The culture theory jungle: Divergence and convergence in models of national culture. *Cambridge handbook of culture, organizations, and work*, 3-22.

Nasheri, H., & Blumstein, A. (2005). *Economic Espionage and Industrial Spying*: Cambridge University Press.
Naughton, J. (2013, September 15). After Edward Snowden's revelations, why trust US cloud providers? Retrieved from https://www.theguardian.com/technology/2013/sep/15/edward-snowden-nsa-cloud-computing
NDR. (2014, January 26). Snowden-Interview: Transcript. Retrieved from http://www.ndr.de/nachrichten/netzwelt/snowden277.html
Neergaard, H., & Ulhøi, J. P. (2007). *Handbook of Qualitative Research Methods in Entrepreneurship*: Edward Elgar.
Neuerer, D. (2013, July 24). Hessens Justizminister für hartes Vorgehen gegen USA [Justice Minister of Hessen for tough action against the USA]. Retrieved from http://www.handelsblatt.com/politik/deutschland/joerg-uwe-hahn-zur-spaehaffaere-hessens-justizminister-fuer-hartes-vorgehen-gegen-usa/8539650.html
Newell, S. J., Belonax, J. J., McCardle, M. W., & Plank, R. E. (2011). The effect of personal relationship and consultative task behaviors on buyer perceptions of salesperson trust, expertise, and loyalty. *Journal of Marketing Theory and Practice, 19*(3), 307-316.
Newell, S. J., Wu, B., Leingpibul, D., & Jiang, Y. (2016). The importance of corporate and salesperson expertise and trust in building loyal business-to-business relationships in China. *Journal of Personal Selling & Sales Management*, 1-14.
Newton, C. (2018, Dec 12). Congress missed another chance to hold big tech accountable. Retrieved from https://www.theverge.com/2018/12/12/18136956/google-hearing-sundar-pichai-congress-bias
Nicholson, C., Compeau, L., & Sethi, R. (2001). The role of interpersonal liking in building trust in long-term channel relationships. *Journal of the Academy of Marketing Science, 29*(1), 3-15. doi:10.1177/0092070301291001
Nieland, A. E. (2006). National security letters and the amended PATRIOT Act. *Cornell L. Rev., 92*, 1201.
Nielson, C. C. (1998). An empirical examination of the role of “closeness” in industrial buyer-seller relationships. *European Journal of Marketing, 32*(5/6), 441-463.
Nikoloff, S. (2013, January 21). Why Europe Doesn’t Trust The Cloud. Retrieved from http://en.sap.info/why-europe-doesnt-trust-the-cloud/85387
NIST. (2011a). *Guidelines on Security and Privacy in Public Cloud Computing* Retrieved from http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf
NIST. (2011b). The NIST Definition of Cloud Computing. *National Institute of Standards and Technology.* Retrieved from http://www.nist.gov/itl/csd/cloud-102511.cfm
Noack, R. (2015, August 14). Germans are so scared of surveillance they microwave their ID cards. Retrieved from https://www.washingtonpost.com/news/worldviews/wp/2015/08/14/germans-are-so-scared-of-surveillance-they-microwave-their-id-cards/
Noor, T. H., Sheng, Q. Z., Maamar, Z., & Zeadally, S. (2016). Managing Trust in the Cloud: State of the Art and Research Challenges. *Computer, 49*(2), 34-45. doi:10.1109/MC.2016.57
Noor, T. H., Sheng, Q. Z., Zeadally, S., & Yu, J. (2013). Trust Management of Services in Cloud Environments: Obstacles and Solutions. *ACM Computing Surveys, 46*(1), 12-12:30. doi:10.1145/2522968.2522980
Nooteboom, B. (2002). *Trust: Forms, Foundations, Functions, Failures and Figures*: Edward Elgar.
Norman, P. M. (2002). Protecting knowledge in strategic alliances: Resource and relational characteristics. *The Journal of High Technology Management Research, 13*(2), 177-202. doi:10.1016/S1047-8310(02)00050-0
Nowak, M. A., & Sigmund, K. (2000). Shrewd investments. *Science, 288*(5467), 819-820.

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic Analysis:Striving to Meet the Trustworthiness Criteria. *International Journal of Qualitative Methods, 16*(1), 1609406917733847. doi:10.1177/1609406917733847

NTT. (2014). *NSA After-shocks: How Snowden has changed ICT decision-makers' approach to the Cloud*. Retrieved from http://nsaaftershocks.com/wp-content/themes/nsa/images/NTTC_Report_WEB.pdf

O'Brien, K. (2016, April 22). U.S. Official: Reason for Optimism on TTIP. Retrieved from https://global.handelsblatt.com/edition/415/ressort/politics/article/u-s-official-reason-for-optimism-on-ttip

O'Keefe, B., & Rapp, N. (2017, February 23). Here are 50 Companies Leading the AI Revolution. Retrieved from http://fortune.com/2017/02/23/artificial-intelligence-companies/

Oakes, G. (1990). The sales process and the paradoxes of trust. *Journal of Business Ethics, 9*(8), 671-679.

Obama, B. (2014, January 17). Remarks by the President on Review of Signals Intelligence. Retrieved from https://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence

Obeidat, M. A., & Turgay, T. (2013). Empirical Analysis for the Factors Affecting the Adoption of Cloud Computing Initiatives by Information Technology Executives. *Journal of Management Research, 5*(1), 152-178.

Obermaier, F., & Schultz, T. (2013, July 12). Wirtschaftsspionage durch amerikanische Geheimdienste: Ausgespäht und ausgenommen [Economic espionage by American intelligence agencies: Spied on and ripped off]. Retrieved from http://www.sueddeutsche.de/politik/wirtschaftsspionage-durch-amerikanische-geheimdienste-ausgespaeht-und-ausgenommen-1.1719795

Oliver, D., & Romm, C. T. (2002). ERP systems in universities: rationale advanced for their adoption *Enterprise resource planning: Global opportunities and challenges* (pp. 43-60): IGI Global.

Oliver, R. L., & Swan, J. E. (1989). Consumer perceptions of interpersonal equity and satisfaction in transactions: a field survey approach. *The Journal of Marketing*, 21-35.

Oltermann, P. (2014, February 4). NSA tapped German ex-chancellor Gerhard Schröder's phone – report. Retrieved from https://www.theguardian.com/world/2014/feb/04/us-nsa-gerhard-schroeder-surveillance

Onwubiko, C. (2010). Security issues to cloud computing *Cloud Computing* (pp. 271-288): Springer.

OpenAI. (2015, December 11). Introducing OpenAI. Retrieved from https://blog.openai.com/introducing-openai/

OpenGroup. (2013, December 16). Cloud Computing for Business : What is Cloud? *The Open Group.* Retrieved from http://www.opengroup.org/cloud/cloud/what.htm

Oppenheim, A. N. (2000). *Questionnaire Design, Interviewing and Attitude Measurement*: Bloomsbury Academic.

Osland, J. S., & Bird, A. (2000). Beyond sophisticated stereotyping: Cultural sensemaking in context. *The Academy of Management Executive, 14*(1), 65-77.

Ouedraogo, W. F., Biennier, F., & Ghodous, P. (2013). Model driven security in a multi-cloud context. *International Journal of Electronic Business Management, 11*(3), 178-190.

Overby, S. (2012, January 20). The Patriot Act and Your Data: Should You Ask Cloud Providers About Protection? *CIO.* Retrieved from http://www.cio.com/article/698432/The_Patriot_Act_and_Your_Data_Should_You_Ask_Cloud_Providers_About_Protection

Oyserman, D., Coon, H. M., & Kemmelmeier, M. (2002). Rethinking individualism and collectivism: evaluation of theoretical assumptions and meta-analyses. *Psychological bulletin, 128*(1), 3.

Palfrey, J. G., & Gasser, U. (2011). *Born digital: Understanding the first generation of digital natives*: ReadHowYouWant. com.

Palmatier, R. W., Dant, R. P., Grewal, D., & Evans, K. R. (2006). Factors Influencing the Effectiveness of Relationship Marketing: A Meta-Analysis. *Journal of Marketing, 70*(4), 136-153. doi:10.2307/30162119

Park, H. (1993). Cultural impact on life insurance penetration: a cross-national analysis. *International Journal of Management, 10*, 342-342.

Park, J.-E., & Holloway, B. B. (2003). Adaptive selling behavior revisited: An empirical examination of learning orientation, sales performance, and job satisfaction. *Journal of Personal Selling & Sales Management, 23*(3), 239-251.

Parkhe, A. (1998a). Building trust in international alliances. *Journal of World Business, 33*(4), 417-437. doi:10.1016/S1090-9516(99)80083-2

Parkhe, A. (1998b). Understanding trust in international alliances. *Journal of World Business, 33*(3), 219-240. doi:10.1016/S1090-9516(99)80072-8

Parkhill, D. F. (1966). *The challenge of the computer utility*: Addison-Wesley Pub. Co.

Pathan, A.-S. K., & Mohammed, M. M. (2015). Building Customer trust in cloud computing with an ICT-enabled global regulatory body. *wireless personal communications, 85*(1), 77-99.

Patil, K., Khatawkar, S., & Dange, A. (2017). Secure Data Sharing in Cloud through Limiting Trust in Third Party/Server. *International Research Journal of Engineering and Technology (IRJET), 4*, 1101-1106.

Pawar, P. S. (2015). *Cloud Broker Based Trust Assessment of Cloud Service Providers.* (Doctoral), City University London. Retrieved from http://openaccess.city.ac.uk/13687/

Payan, J. M., & McFarland, R. G. (2005). The Effects of Influence Strategies and Dependence on Satisfaction. *Journal of Marketing Channels, 13*(1), 3-20. doi:10.1300/J049v13n01_02

Pearson, S. (2009). *Taking account of privacy when designing cloud computing services.* Paper presented at the Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing.

Pearson, S. (2012). Privacy, Security and Trust in Cloud Computing. In S. Pearson & G. Yee (Eds.), *Privacy and Security for Cloud Computing*. London: Springer.

Pechardscheck, S., & Schiefer, C. (2012). *In Cloud we trust?* Retrieved from

Peer1. (2014). The Impact of the NSA on Hosting Decision Makers in the UK and Canada. Retrieved from http://go.peer1.com/rs/peer1/images/Peer1-Report-NSA-Survey-NA.pdf

Perlroth, N., Larson, J., & Shane, S. (2013, September 5). N.S.A. Able to Foil Basic Safeguards of Privacy on Web. Retrieved from http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html

Peters, H. P., Lang, J. T., Sawicka, M., & Hallman, W. K. (2007). Culture and technological innovation: Impact of institutional trust and appreciation of nature on attitudes towards food biotechnology in the USA and Germany. *International Journal of Public Opinion Research, 19*(2), 191-220.

Peters, L. D., Pressey, A. D., Vanharanta, M., & Johnston, W. J. (2013). Constructivism and critical realism as alternative approaches to the study of business networks: Convergences and divergences in theory and in research practice. *Industrial Marketing Management, 42*(3), 336-346. doi:http://dx.doi.org/10.1016/j.indmarman.2013.02.003

Pettersson, E. (2016, March 3). Microsoft, Google Join Rivals to Back Apple in FBI Fight. Retrieved from http://www.bloomberg.com/news/articles/2016-03-03/apple-supporters-weigh-in-from-big-tech-to-a-terror-victim

Phillips, M. (2018). International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR). *Human genetics*, 1-8.

Pilkington, E. (2013, March 15). FBI's demands for private data struck down by federal court. *The Guardian.* Retrieved from http://www.theguardian.com/world/2013/mar/15/court-strikes-down-fbi-data-demands/print

Pincus, W. (2013, December 19). Snowden still holding 'keys to the kingdom'. *The Washington Post.* Retrieved from http://www.washingtonpost.com/world/national-security/snowden-still-holding-keys-to-the-kingdom/2013/12/18/b91d29a2-6761-11e3-8b5b-a77187b716a3_story.html

Pinsent Masons. (2018, May 25). New Data Protection Act finalised in the UK. Retrieved from https://www.out-law.com/en/articles/2018/may/new-data-protection-act-finalised-uk/

Pirrone, M., & Trainor, J. E. (2013). Cloud Computing, Social Media, and Confidentiality. *The CPA Journal, 83*(11), 58-60,62.

Pirson, M. (2007). *Facing the Trust Gap: Measuring and Building Trust in Organizations.* University of St. Gallen.

Plank, R. E., Reid, D. A., & Ellen Bolman, P. (1999). Perceived trust in business-to-business sales: A new measure. *The Journal of Personal Selling & Sales Management, 19*(3), 61-71.

Png, I. P., Tan, B. C., & Wee, K.-L. (2001). Dimensions of national culture and corporate adoption of IT infrastructure. *IEEE Transactions on Engineering Management, 48*(1), 36-45.

Poitras, L., Rosenbach, M., & Stark, H. (2014, March 29). GCHQ and NSA Targeted Private German Companies and Merkel. Retrieved from http://www.spiegel.de/international/germany/gchq-and-nsa-targeted-private-german-companies-a-961444.html

Portal, S., Abratt, R., & Bendixen, M. (2018). The role of brand authenticity in developing brand trust. *Journal of Strategic Marketing*, 1-16.

Porter, L. W., Lawler, E. E., & Hackman, J. R. (1975). *Behavior in Organizations*: McGraw-Hill.

Porter, N., Garms, J., & Simakov, S. (2018, May 3). Introducing Asylo: an open-source framework for confidential computing. Retrieved from https://cloud.google.com/blog/products/gcp/introducing-asylo-an-open-source-framework-for-confidential-computing

Posey, C., Lowry, P. B., Roberts, T. L., & Ellis, T. S. (2010). Proposing the online community self-disclosure model: the case of working professionals in France and the UK who use online communities. *European Journal of Information Systems, 19*(2), 181-195.

Pothukuchi, V., Damanpour, F., Choi, J., Chen, C. C., & Park, S. H. (2002). National and organizational culture differences and international joint venture performance. *Journal of international Business studies, 33*(2), 243-265.

Pring-Mill, D. (2018, Jun 4). Why We Need Tech-Savvy Politicians. Retrieved from https://www.dmnews.com/customer-experience/article/13034502/why-we-need-techsavvy-politicians

Priyam, P. (2018). *Cloud Security Automation: Get to grips with automating your cloud security on AWS and OpenStack*: Packt Publishing.

Prodhan, G., & Davenport, C. (2013, June 8). US surveillance revelations deepen European fears. *Reuters.* Retrieved from http://www.reuters.com/article/2013/06/08/us-europe-surveillance-prism-idUSBRE95614M20130608

Prosser, W. L. (1960). Privacy. *California Law Review, 48*(3), 383-423.

Pruitt, D. G. (1981). *Negotiation behavior* (Vol. 47): Academic Press New York.

Punch, K. F. (2009). *Introduction to Research Methods in Education*: SAGE.

Putnam, R. D. (2000). Bowling alone: America's declining social capital *Culture and politics* (pp. 223-234): Springer.

PwC. (2011). *Cloud Computing in the Middle Market: Experiences, Advantages and Challenges* Retrieved from http://www.pwc.de/en/mittelstand/cloud-computing-im-mittelstand.jhtml
PwC. (2013a). *Cloud Computing: Evolution in the Cloud [Cloud Computing: Evolution in the Cloud]*: PricewaterhouseCoopers.
PwC. (2013b). *Wirtschaftskriminalität und Unternehmenskultur 2013 [Economic Crime and Corporate Culture 2013]*: PricewaterhouseCoopers & Martin-Luther-Universität Halle-Wittenberg.
PwC. (2014). *Wirtschaftskriminalität und Compliance in der Automobilindustrie [Economic crime and compliance in the automotive industry]*: PricewaterhouseCoopers.
Qi, C., & Chau, P. Y. (2013). Investigating the roles of interpersonal and interorganizational trust in IT outsourcing success. *Information Technology & People, 26*(2), 120-145.
Rahn, C. (2011, September 14). Deutsche Telekom Wants `German Cloud' to Shield Data From U.S. *Bloomberg.* Retrieved from http://www.bloomberg.com/news/2011-09-13/deutsche-telekom-wants-german-cloud-to-shield-data-from-u-s-.html
Rahn, C. (2012, January 17). Europe Won't Let U.S. Dominate Cloud With Rules to Curb HP: Tech. Retrieved from http://www.bloomberg.com/news/2012-01-17/europe-won-t-let-u-s-dominate-cloud-with-rules-to-curb-hp-tech.html
Ramsey, R. P., & Sohi, R. S. (1997). Listening to your customers: The impact of perceived salesperson listening behavior on relationship outcomes. *Journal of the Academy of Marketing Science, 25*(2), 127.
Rappeport, A. (2018, Aug 21). US companies warn additional China tariffs will cripple their business and hurt customers. Retrieved from https://www.independent.co.uk/news/world/americas/us-china-tariffs-business-damage-trade-economy-trump-imports-exports-goods-a8501361.html
Razzaque, M. A., & Boon, T. G. (2003). Effects of Dependence and Trust on Channel Satisfaction, Commitment and Cooperation. *Journal of Business-to-Business Marketing, 10*(4), 23-48. doi:10.1300/J033v10n04_02
Reding, V. (2011, December 7). Privacy in the Cloud: Data Protection and Security in Cloud Computing. *European Commission - SPEECH/11/859.* Retrieved from http://europa.eu/rapid/press-release_SPEECH-11-859_en.htm
Reding, V. (2013a, September 17). Data protection reform: restoring trust and building the digital single market. *European Commission - SPEECH/13/720.* Retrieved from http://europa.eu/rapid/press-release_SPEECH-13-720_en.htm
Reding, V. (2013b, June 14). PRISM scandal: The data protection rights of EU citizens are non-negotiable. *European Commission - SPEECH/13/536.* Retrieved from http://europa.eu/rapid/press-release_SPEECH-13-536_en.htm
Reding, V. (2013c, July 3). U.S. and EU Member State surveillance programmes: National security does not mean that anything goes. *European Commission - SPEECH/13/607.* Retrieved from http://europa.eu/rapid/press-release_SPEECH-13-607_en.htm
Reding, V. (2014, January 15). Future of the Safe Harbour Agreement in the light of the NSA affair. *European Commission - SPEECH/14/27.* Retrieved from http://europa.eu/rapid/press-release_SPEECH-14-27_en.htm
Reform Government Surveillance. (2013). An open letter to Washington. Retrieved from https://www.reformgovernmentsurveillance.com
Reitman, R. (2015, April 30). The New USA Freedom Act: A Step in the Right Direction, but More Must Be Done. Retrieved from https://www.eff.org/deeplinks/2015/04/new-usa-freedom-act-step-right-direction-more-must-be-done
Rennie, S. (2010). Legal Implications of Working in the Cloud. *Information Management, 44*(5), HT11-HT12,HT14,HT16.
Restore the Fourth. (2016, September 6). Opposing unconstitutional mass government surveillance. Retrieved from https://restorethe4th.com/

Reuters. (2008, August 29). Trump renews attack against technology companies. Retrieved from https://www.reuters.com/article/us-usa-trump-tech/trump-renews-attack-against-technology-companies-idUSKCN1LE2FK
Reynolds, M. (1998). Reflection and critical reflection in management learning. *Management learning, 29*(2), 183-200.
Ries, S. (2009). *Trust in ubiquitous computing.* (Ph.D.), Technische Universität Darmstadt, Darmstadt.
Riessman, C. K. (1993). *Narrative analysis* (Vol. 30): Sage.
Rittinghouse, J. W., & Ransome, J. F. (2017). *Cloud Computing: Implementation, Management, and Security*: CRC Press.
Roberts II, J. C., & Al-Hamdani, W. (2011). *Who can you trust in the cloud?: a review of security issues within cloud computing*. Paper presented at the Proceedings of the 2011 Information Security Curriculum Development Conference, Kennesaw, Georgia.
Robinson, S. L. (1996). Trust and Breach of the Psychological Contract. *Administrative science quarterly, 41*(4), 574-599. doi:10.2307/2393868
Rodriguez, J. T., & Obradovac, I. (2017). Comparative study on user's perception of privacy issues on Facebook: Young adults vs. adults in Sweden.
Rohrmann, C. A., Cunha, S. R., & Falci, J. (2015). Some legal aspects of cloud computing contracts. *J. Int't Com. L. & Tech., 10*, 37.
Román, S., & Iacobucci, D. (2010). Antecedents and consequences of adaptive selling confidence and behavior: a dyadic analysis of salespeople and their customers. *Journal of the Academy of Marketing Science, 38*(3), 363-382.
Rose, S., Spinks, N., & Canhoto, A. I. (2014). *Management Research: Applying the Principles*: Taylor & Francis.
Rossi, A. (2018). How the Snowden Revelations Saved the EU General Data Protection Regulation. *The International Spectator, 53*(4), 95-111.
Rothman, L. (2016, March 28). The Long History Behind Donald Trump's 'America First' Foreign Policy. Retrieved from http://time.com/4273812/america-first-donald-trump-history/
Rothstein, B., & Stolle, D. (2008). The state and social capital: An institutional theory of generalized trust. *Comparative politics, 40*(4), 441-459.
Rotter, J. B. (1967). A new scale for the measurement of interpersonal trust. *Journal of Personality, 35*(4), 651-665. doi:10.1111/j.1467-6494.1967.tb01454.x
Rotter, J. B., Chance, J. E., & Phares, E. J. (1972). *Applications of a social learning theory of personality*: Holt, Rinehart and Winston.
Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. *Academy of management review, 23*(3), 393-404.
Rowley, J. (2012). Conducting research interviews. *Management Research Review, 35*(3/4), 260-271. doi:10.1108/01409171211210154
Ruparelia, N. B. (2016). *Cloud Computing*: MIT Press.
Rushe, D. (2013, September 12). Zuckerberg: US government 'blew it' on NSA surveillance. Retrieved from https://www.theguardian.com/technology/2013/sep/11/yahoo-ceo-mayer-jail-nsa-surveillance
Russinovich, M. (2017, Sep 14). Introducing Azure confidential computing. Retrieved from https://azure.microsoft.com/en-us/blog/introducing-azure-confidential-computing/
Rutherford, B. (2007). *The Differing Effects of Satisfaction, Trust, and Commitment on Buyer's Behavioral Loyalty: A Study into the Buyer-Salesperson and Buyer-Selling Firm Relationship in a Business-to-Business Context.* Georgia State University.
Ryu, S., Park, J. E., & Min, S. (2007). Factors of determining long-term orientation in interfirm relationships. *Journal of Business Research, 60*(12), 1225-1233. doi:10.1016/j.jbusres.2006.09.031
Sabel, C. F. (1993). Studied trust: Building new forms of cooperation in a volatile economy. *Human Relations, 46*(9), 1133.

Sabherwal, R. (1999). The role of trust in outsourced IS development projects. *Communications of the ACM, 42*(2), 80-86.
Sako, M. (1992). *Price, Quality and Trust: Inter-firm Relations in Britain and Japan*: Cambridge University Press.
Sako, M. (1998). Does trust improve business performance? *Oxford University Press, Oxford*, 88-117.
Sako, M., & Helper, S. (1998). Determinants of trust in supplier relations: Evidence from the automotive industry in Japan and the United States. *Journal of Economic Behavior & Organization, 34*(3), 387-417. doi:10.1016/S0167-2681(97)00082-6
Salesforce. (2015, July 2). Salesforce Customer and Partner Momentum Accelerates in Germany, Creating Positive Impact On German Economy. Retrieved from http://investor.salesforce.com/about-us/investor/investor-news/investor-news-details/2015/Salesforce-Customer-and-Partner-Momentum-Accelerates-in-Germany-Creating-Positive-Impact-On-German-Economy/default.aspx
Salesforce. (2016, July 12). Announcing Bring Your Own Key Encryption for the Salesforce Platform. Retrieved from https://www.salesforce.com/blog/2016/07/bring-your-own-key-encryption-salesforce-platform.html
Sambrook, S., & Stewart, J. (2008). Developing critical reflection in professional focused doctorates: a facilitator's perspective. *Journal of European Industrial Training, 32*(5), 359-373.
Sampson, H. (2004). Navigating the waves: the usefulness of a pilot in qualitative research. *Qualitative Research, 4*(3), 383-402.
Sapsford, R. (2006). Methodology. In V. Jupp (Ed.), *The Sage Dictionary of Social Research Methods*: Sage.
Sarstedt, M., & Mooi, E. (2011). *A Concise Guide to Market Research: The Process, Data, and Methods Using IBM SPSS Statistics*: Springer.
Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research Methods for Business Students*: Pearson Education.
Sayer, P. (2012, September 6). French Sovereign Wealth Funds Invests in Two Local Cloud Computing Providers. *CIO.* Retrieved from http://www.cio.com/article/715523/French_Sovereign_Wealth_Funds_Invests_in_Two_Local_Cloud_Computing_Providers
Scahill, J., & Begley, J. (2015, February 19). The Great SIM Heist – How Spies Stole the Keys to the Encryption Castle. Retrieved from https://theintercept.com/2015/02/19/great-sim-heist/
Schallbruch, M., & Skierka, I. (2018). The German View on Cybersecurity *Cybersecurity in Germany* (pp. 5-14): Springer.
Schechner, S. (2016, August 4). U.S. Tech Firms Dominate Cloud Services in Western Europe. Retrieved from https://www.wsj.com/articles/u-s-tech-firms-dominate-cloud-services-in-western-europe-1470303004
Schein, E. H. (1985). *Organizational Culture and Leadership*. San Francisco: Jossey-Bass.
Schein, E. H. (2010). *Organizational Culture and Leadership*: John Wiley & Sons.
Schlenker, B. R., Helm, B., & Tedeschi, J. T. (1973). The effects of personality and situational variables on behavioral trust. *Journal of Personality and Social Psychology, 25*(3), 419-427. doi:10.1037/h0034088
Schlosser, A. E., White, T. B., & Lloyd, S. M. (2006). Converting web site visitors into buyers: how web site investment increases consumer trusting beliefs and online purchase intentions. *Journal of Marketing, 70*(2), 133-148.
Schmidt, M. J., & Hollensen, S. (2006). *Marketing research: an international approach*: Prentice Hall/Financial Times.
Schneider, S., & Sunyaev, A. (2016). Determinant factors of cloud-sourcing decisions: reflecting on the IT outsourcing literature in the era of cloud computing. *Journal of Information Technology, 31*(1), 1-31.

Schneider, S. C., & Barsoux, J.-L. (2003). *Managing across cultures*: Pearson Education.
Schneier, B. (2013, July 31). NSA secrets kill our trust. Retrieved from http://edition.cnn.com/2013/07/31/opinion/schneier-nsa-trust/index.html
Schoorman, F. D., Mayer, R. C., & Davis, J. H. (2007). An integrative model of organizational trust: Past, present, and future. *Academy of management review, 32*(2), 344-354.
Schurr, P. H., & Ozanne, J. L. (1985). Influences on exchange processes: buyers' preconceptions of a seller's trustworthiness and bargaining toughness. *Journal of Consumer Research, 11*(4), 939-953.
Schwandt, T. A. (2000). Three epistemological stances for qualitative inquiry: Interpretivism, hermeneutics, and social constructionism. *Handbook of qualitative research, 2*, 189-213.
Schwartz, S. H. (1992). Universals in the content and structure of values: Theoretical advances and empirical tests in 20 countries *Advances in experimental social psychology* (Vol. 25, pp. 1-65): Elsevier.
Schwegler, U. (2006). *Trust building processes within German–Indonesian cooperation.* Paper presented at the 22nd EGOS Colloquium.
Scott, M. (2014a, June 11). European Firms Turn Privacy Into Sales Pitch. Retrieved from http://bits.blogs.nytimes.com/2014/06/11/european-firms-turn-privacy-into-sales-pitch/
Scott, M. (2014b, December 24). Ireland Lends Support to Microsoft in Email Privacy Case. Retrieved from http://bits.blogs.nytimes.com/2014/12/24/ireland-lends-support-to-microsoft-in-email-privacy-case/
Scott, M. (2016, October 3). U.S. Tech Giants Are Investing Billions to Keep Data in Europe. Retrieved from https://www.nytimes.com/2016/10/04/technology/us-europe-cloud-computing-amazon-microsoft-google.html?_r=0
Seddon, J. J., & Currie, W. L. (2013). Cloud computing and trans-border health data: Unpacking US and EU healthcare regulation and compliance. *Health policy and technology, 2*(4), 229-241.
Seidman, I. (2006). *Interviewing as qualitative research: a guide for researchers in education and the social sciences*: Teachers College Press.
Seligman, A. B. (2000). *The Problem of Trust*: Princeton University Press.
Selnes, F. (1998). Antecedents and consequences of trust and satisfaction in buyer-seller relationships. *European Journal of Marketing, 32*(3/4), 305-322.
Selvaraj, A., & Sundararajan, S. (2017). Evidence-based trust evaluation system for cloud services using fuzzy logic. *International Journal of Fuzzy Systems, 19*(2), 329-337.
Sensenbrenner, J. (2013, June 6). Author of Patriot Act: FBI's FISA Order is Abuse of Patriot Act. Retrieved from http://sensenbrenner.house.gov/news/documentsingle.aspx?DocumentID=337001
Seppänen, R., Blomqvist, K., & Sundqvist, S. (2007). Measuring inter-organizational trust—a critical review of the empirical research in 1990–2003. *Industrial Marketing Management, 36*(2), 249-265. doi:10.1016/j.indmarman.2005.09.003
Severin, T. (2014, June 26). German government cancels Verizon contract in wake of U.S. spying row. Retrieved from http://www.reuters.com/article/us-germany-security-verizon-idUSKBN0F11WJ20140626
Severson, D. (2015). American Surveillance of Non-US Persons: Why New Privacy Protections Offer Only Cosmetic Change. *Harv. Int'l LJ, 56*, 465.
Shackelford, S. J., & Russell, S. (2014). Above the Cloud: Enhancing Cybersecurity in the Aerospace Sector. *FIU L. Rev., 10*, 635.
Shahani, A. (2014, June 5). A Year After Snowden, U.S. Tech Losing Trust Overseas. Retrieved from http://www.npr.org/sections/alltechconsidered/2014/06/05/318770896/a-year-after-snowden-u-s-tech-losing-trust-overseas?sc=17&f=1001

Shaikh, A. (2018). Shadow-IT system and Insider Threat: Opportunity as a Situational Perspective.
Shankar, V., Urban, G. L., & Sultan, F. (2002). Online trust: a stakeholder perspective, concepts, implications, and future directions. *The Journal of Strategic Information Systems, 11*(3–4), 325-344. doi:10.1016/S0963-8687(02)00022-7
Shapiro, S. P. (1987). The social control of impersonal trust. *American journal of Sociology*, 623-658.
Sharma, A. (1990). The Persuasive Effect of Salesperson Credibility: Conceptual and Empirical Examination. *The Journal of Personal Selling and Sales Management, 10*(4), 71-80. doi:10.2307/40471837
Sharma, P., Sood, S. K., & Kaur, S. (2011). Security issues in cloud computing *High Performance Architecture and Grid Computing* (pp. 36-45): Springer.
Shaw, R. B. (1997). *Trust in the Balance: Building Successful Organizations on Results, Integrity, and Concern*: Wiley.
Shenkar, O. (2001). Cultural distance revisited: Towards a more rigorous conceptualization and measurement of cultural differences. *Journal of international Business studies, 32*(3), 519-535.
Shepherd, C. D., Gardial, S. F., Johnson, M. G., & Rentz, J. O. (2006). Cognitive insights into the highly skilled or expert salesperson. *Psychology & Marketing, 23*(2), 115-138.
Sherman, G. (2018, Apr 2). “TRUMP IS LIKE, ‘HOW CAN I F--K WITH HIM?’”: TRUMP’S WAR WITH AMAZON (AND THE WASHINGTON POST) IS PERSONAL. Retrieved from https://www.vanityfair.com/news/2018/04/trump-war-with-amazon-and-the-washington-post-is-personal
Sherr, I. (2017, February 2). Here's what tech has to say about Trump's immigration ban. Retrieved from https://www.cnet.com/news/tech-apple-google-facebook-uber-amazon-airbnb-tesla-microsoft-trump-immigration-ban/
Shih, G., & Carsten, P. (2014, August 15). Apple begins storing users' personal data on servers in China. Retrieved from http://www.reuters.com/article/us-apple-data-china-idUSKBN0GF0N720140815
Shoemaker, M. E., & Johlke, M. C. (2002). An examination of the antecedents of a crucial selling skill: asking questions. *Journal of Managerial Issues*, 118-131.
Sia, C. L., Lim, K. H., Leung, K., Lee, M. K., Huang, W. W., & Benbasat, I. (2009). Web strategies to promote internet shopping: is cultural-customization needed? *Mis Quarterly*, 491-512.
Sidhu, J., & Singh, S. (2017). Improved topsis method based trust evaluation framework for determining trustworthiness of cloud service providers. *Journal of Grid Computing, 15*(1), 81-105.
Silic, M., & Back, A. (2014). Shadow IT–A view from behind the curtain. *Computers & Security, 45*, 274-283.
Silverman, D. (2009). *Doing Qualitative Research*: SAGE.
Silverman, D. (2013). *Doing Qualitative Research: A Practical Handbook*: SAGE.
Silverman, D., & Marvasti, A. (2008). *Doing Qualitative Research: A Comprehensive Guide*: SAGE.
Singh, J. P. (1990). Managerial culture and work-related values in India. *Organization Studies, 11*(1), 075-101.
Sitkin, S. B., & Roth, N. L. (1993). Explaining the Limited Effectiveness of Legalistic "Remedies" for Trust/ Distrust. *Organization Science, 4*(3), 367-392. doi:10.2307/2634950
Smale, A. (2013, October 24). Indignation Over U.S. Spying Spreads in Europe. Retrieved from http://www.nytimes.com/2013/10/25/world/europe/indignation-over-us-spying-spreads-in-europe.html

Smircich, L. (1983). Concepts of culture and organizational analysis. *Administrative science quarterly*, 339-358.

Smith, B. (2018, Apr 3). The CLOUD Act is an important step forward, but now more steps need to follow. Retrieved from https://blogs.microsoft.com/on-the-issues/2018/04/03/the-cloud-act-is-an-important-step-forward-but-now-more-steps-need-to-follow/

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: measuring individuals' concerns about organizational practices. *Mis Quarterly*, 167-196.

Smith, J., & Wiest, D. (2005). The uneven geography of global civil society: National and global influences on transnational association. *Social Forces, 84*(2), 621-652.

Smith, J. B., & Barclay, D. W. (1997). The effects of organizational differences and trust on the effectiveness of selling partner relationships. *Journal of Marketing, 61*(1), 3-21.

Smith, L. R., & Schwegler, U. (2010). The role of trust in international cooperation in crisis areas: of German and US-American NGO partnership strategies. In M. N. K. Saunders, D. Skinner, G. Dietz, N. Gillespie, & R. J. Lewicki (Eds.), *Organizational trust: A cultural perspective* (pp. 281).

Smith, R. (2009). Computing in the cloud. *Research Technology Management, 52*(5), 65-68.

Sobel, J. (2002). Can We Trust Social Capital? *Journal of Economic Literature, 40*(1), 139-154. doi:10.2307/2698596

Sofroniou, A. (2007). *Moral Philosophy, from Hippocrates to the 21st Aeon*: Lulu.com.

Solon, O. (2016, August 16). Hacking group auctions 'cyber weapons' stolen from NSA. Retrieved from https://www.theguardian.com/technology/2016/aug/16/shadow-brokers-hack-auction-nsa-malware-equation-group

Solon, O. (2017, April 24). Alibaba founder Jack Ma: AI will cause people ‘more pain than happiness’. Retrieved from https://www.theguardian.com/technology/2017/apr/24/alibaba-jack-ma-artificial-intelligence-more-pain-than-happiness

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review, 154*(3), 477-564.

Soltani, A., & DeLong, M. (2013, December 5). GHOSTMACHINE: The NSA's cloud analytics platform. *The Washington Post.* Retrieved from http://apps.washingtonpost.com/g/page/world/ghostmachine-the-nsas-cloud-analytics-platform/644/

Soltani, A., Peterson, A., & Gellman, B. (2013, December 10). NSA uses Google cookies to pinpoint targets for hacking [Web log post]. *The Washington Post*. Retrieved from http://www.washingtonpost.com/blogs/the-switch/wp/2013/12/10/nsa-uses-google-cookies-to-pinpoint-targets-for-hacking/

Søndergaard, M. (1994). Research note: Hofstede's consequences: a study of reviews, citations and replications. *Organization Studies, 15*(3), 447-456.

Spekman, R. E. (1988). Strategic Supplier Selection: Understanding Long-Term Buyer Relationships. *Business Horizons, 31*(4), 75.

Spiegel Online. (2013, July 10). Merkel Speaks: Chancellor Defends Intelligence Monitoring. Retrieved from http://www.spiegel.de/international/germany/german-chancellor-merkel-defends-work-of-intelligence-agencies-a-910491.html

Spiegel Online. (2015a, April 29). BDI-Chef über BND-Affäre: "Verhältnis zwischen Staat und Industrie ist erheblich belastet" [Head of BDI on BND affair: "Relationship between state and industry is significantly strained"]. Retrieved from http://www.spiegel.de/wirtschaft/soziales/bnd-affaere-bdi-kritisiert-bundesregierung-scharf-a-1031290.html

Spiegel Online. (2015b, June 5). BND-Mitarbeiter erhärtet Verdacht auf Wirtschaftsspionage [BND employees confirmed suspicion of economic espionage]. Retrieved from http://www.spiegel.de/politik/deutschland/bnd-affaere-verdacht-auf-wirtschaftsspionage-erhaertet-a-1037370.html

Srinivasan, M., & Srivastava, P. (2012). The Role of the Salesperson in Building Trust and Collaboration in Buyer-Seller Relationships. *Supply Chain Forum: International Journal, 13*(2), 22-38.

Srinivasan, R. (2017). *Whose Global Village?: Rethinking How Technology Shapes Our World*: NYU Press.

Srite, M., & Karahanna, E. (2006). The role of espoused national cultural values in technology acceptance. *Mis Quarterly*, 679-704.

Staten, J. (2009, October 14). Cloud is defined, now stop the cloudwashing [Web log post]. *Forrester Research, Inc.* Retrieved from http://blogs.forrester.com/james_staten/09-10-14-cloud_defined_now_stop_cloudwashing

Staten, J. (2013, August 14). The Cost of PRISM Will Be Larger Than ITIF Projects. Retrieved from http://blogs.forrester.com/james_staten/13-08-14-the_cost_of_prism_will_be_larger_than_itif_projects

Steeves, V., & Webster, C. (2008). Closing the barn door: The effect of parental supervision on Canadian children's online privacy. *Bulletin of Science, Technology & Society, 28*(1), 4-19.

Steinhaus, I. (2013, September 27). Das Schlüsselwort ist Vertrauen [The key word is trust]. Retrieved from http://www.it-zoom.de/it-mittelstand/e/das-schluesselwort-ist-vertrauen-7421/

Stempel, J. (2016, July 14). Microsoft wins landmark appeal over seizure of foreign emails. Retrieved from http://www.reuters.com/article/us-microsoft-usa-warrant-idUSKCN0ZU1RJ

Stempel, J. (2017, January 24). Microsoft victory in overseas email seizure case is upheld. Retrieved from http://uk.reuters.com/article/us-microsoft-usa-warrant-idUKKBN1581YQ

Stewart, E. (2018, Apr 10). Lawmakers seem confused about what Facebook does — and how to fix it. Retrieved from https://www.vox.com/policy-and-politics/2018/4/10/17222062/mark-zuckerberg-testimony-graham-facebook-regulations

Stieninger, M., & Nedbal, D. (2014). *Diffusion and acceptance of cloud computing in SMEs: towards a valence model of relevant factors.* Paper presented at the System Sciences (HICSS), 2014 47th Hawaii International Conference on.

Stiglitz, J. E. (2013, December 21). In No One We Trust. Retrieved from http://opinionator.blogs.nytimes.com/2013/12/21/in-no-one-we-trust

Stohr, G. (2017, Oct 16). Microsoft Email-Access Fight With U.S. Gets Top Court Review. Retrieved from https://www.bloomberg.com/news/articles/2017-10-16/microsoft-email-access-fight-with-u-s-gets-supreme-court-review

Stohr, G. (2018, Mar 31). Justice Department Asks Court to Drop Microsoft Email Case. Retrieved from https://www.bloomberg.com/news/articles/2018-03-31/justice-department-asks-high-court-to-drop-microsoft-email-case

Stölzel, T. (2011, August 6). Google-Server in Europa vor US-Regierung nicht sicher [Google's servers in Europe not safe from US government]. *Wirtschaftswoche.* Retrieved from http://www.wiwo.de/politik/ausland/datenspeicherung-google-server-in-europa-vor-us-regierung-nicht-sicher/5156042.html

Stop Watching Us. (2013, October 26). On October 26th thousands of you gathered on the steps of the capitol and sent a clear message to Congress: Stop Watching Us. Retrieved from https://rally.stopwatching.us/

Straub, D., Keil, M., & Brenner, W. (1997). Testing the technology acceptance model across cultures: A three country study. *Information & Management, 33*(1), 1-11.

Straub, D., Loch, K., Evaristo, R., Karahanna, E., & Srite, M. (2002). Toward a theory-based measurement of culture. *Journal of Global Information Management (JGIM), 10*(1), 13-23.

Strong, D. M., & Volkoff, O. (2004). A roadmap for enterprise system implementation. *Computer, 37*(6), 22-29.

Strutton, D., Pelton, L. E., & Tanner Jr, J. F. (1996). Shall we gather in the garden: The effect of ingratiatory behaviors on buyer trust in salespeople. *Industrial Marketing Management, 25*(2), 151-162. doi:10.1016/0019-8501(95)00074-7

Stuart, K., & Bromage, D. (2010). Current state of play: records management and the cloud. *Records Management Journal, 20*(2), 217-225. doi:10.1108/09565691011064340

Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications, 34*(1), 1-11.

Sujan, H., Weitz, B. A., & Kumar, N. (1994). Learning orientation, working smart, and effective selling. *Journal of Marketing, 58*(3), 39-52.

Sung-Joon, Y. (2002). The antecedents and consequences of trust in online-purchase decisions. *Journal of Interactive Marketing, 16*(2), 47-63.

Sverdlik, Y. (2017, 3 Mar). Here are the Submarine Cables Funded by Cloud Giants. Retrieved from http://www.datacenterknowledge.com/archives/2017/03/03/here-are-the-submarine-cables-funded-by-cloud-giants/

Swan, J. E., Bowers, M. R., & Richardson, L. D. (1999). Customer Trust in the Salesperson: An Integrative Review and Meta-Analysis of the Empirical Literature. *Journal of Business Research, 44*(2), 93-107. doi:http://dx.doi.org/10.1016/S0148-2963(97)00244-0

Swan, J. E., & Nolan, J. J. (1985). Gaining Customer Trust: A Conceptual Guide for the Salesperson. *The Journal of Personal Selling and Sales Management, 5*(2 (Nov)), 39-48. doi:10.2307/20832402

Swan, J. E., Trawick, I. F., Jr., Rink, D. R., & Roberts, J. J. (1988). Measuring Dimensions of Purchaser Trust of Industrial Salespeople. *The Journal of Personal Selling and Sales Management, 8*(1), 1-9. doi:10.2307/20832436

Swan, J. E., Trawick, I. F., & Silva, D. W. (1985). How Industrial Salespeople Gain Customer Trust. *Industrial Marketing Management, 14*(3 (Aug)), 203.

Swisher, K. (2015, 15 Feb). White House. Red Chair. Obama Meets Swisher. Retrieved from http://www.recode.net/2015/2/15/11559056/white-house-red-chair-obama-meets-swisher

SZ. (2017, 9 Jan). Merkel: Deutschland droht, digitales Entwicklungsland zu werden [Merkel: Germany could become a digital developing country]. Retrieved from http://www.sueddeutsche.de/politik/digitalisierung-merkel-deutschland-droht-digitales-entwicklungsland-zu-werden-1.3326389

Sztompka, P. (1999). *Trust: A Sociological Theory*: Cambridge University Press.

T-Systems. (2017, Mar 16). Sales of Microsoft Cloud Deutschland launch at Deutsche Telekom. Retrieved from https://www.telekom.com/en/media/media-information/archive/sales-of-microsoft-cloud-deutschland-launch-at-deutsche-telekom-487998

Tam, J. L., & Wong, Y. (2001). Interactive selling: a dynamic framework for services. *Journal of Services Marketing, 15*(5), 379-396.

Tang, M., Dai, X., Liu, J., & Chen, J. (2017). Towards a trust evaluation middleware for cloud service selection. *Future Generation computer systems, 74*, 302-312.

Tassabehji, R., & Hackney, R. (2016). 'Hey You? Get Off My Cloud': Evaluation of Cloud Service Models for Business Value within Pharma X. *Journal of Advances in Management Sciences & Information Systems, 2*, 48-52.

Tatje, C. (2013, Jan 3). Ich muss löschen können. Retrieved from https://www.zeit.de/2013/02/Big-Data-Interview-Albrecht

Taylor, P. (2011, August 2). Privacy concerns slow cloud adoption. Retrieved from http://www.ft.com/intl/cms/s/0/c970e6ee-bc7e-11e0-adac-00144feabdc0.html#axzz2F9xFpE6p

Taylor, P. (2013, August 5). Cloud computing industry could lose up to $35bn on NSA disclosures. *The Financial Times.* Retrieved from http://www.ft.com/intl/cms/s/0/9f02b396-fdf0-11e2-a5b1-00144feabdc0.html#axzz2z7XOXPUy

Techconsult. (2012). *Cloud-Bericht 2012-05-07: Handel liegt bei Cloud-Nutzung vorn [Cloud report 2012-05-07: Trade is ahead in cloud usage]*. Retrieved from

Techconsult. (2013a). *Cloud-Bericht 2013-06-06: CRM aus der Cloud im Mittelstands Fokus [Cloud Report 2013-06-06: CRM from the cloud in the SME focus]*. Retrieved from

Techconsult. (2013b). *Cloud-Bericht 2013-07-02: Mit Standardisierung und Beratung in die Cloud [Cloud Report 2013-07-02: With standardization and consulting in the cloud]*. Retrieved from

Techconsult. (2013c). *Cloud-Bericht 2013-08-06: PRISM und die Cloud – der Blick nach vorn [Cloud Report 2013-08-06: PRISM and the Cloud - the look ahead]*. Retrieved from

Techconsult. (2013d). *Cloud-Bericht 2013-09-26: Cloud Technologie trotz PRISM vorn [Cloud report 2013-09-26: Cloud technology despite PRISM ahead]*. Retrieved from Kassel:

Telecompaper. (2012a, September 7). Orange, Thales announce Cloudwatt cloud computing venture. *Telecom.paper BV.* Retrieved from http://www.telecompaper.com/news/orange-thales-announce-cloudwatt-cloud-computing-venture--894561

Telecompaper. (2012b, September 5). SFR, Bull launch Numergy cloud computing venture. *Telecom.paper BV.* Retrieved from http://www.telecompaper.com/news/sfr-bull-launch-numergy-cloud-computing-venture--893979

Thatcher, J. B., Stepina, L. P., Srite, M., & Liu, Y. (2003). Culture, overload and personal innovativeness with information technology: Extending the nomological net. *Journal of Computer Information Systems, 44*(1), 74-81.

The Day We Fight Back. (2014, 11 Feb). The Day We Fight Back Against Mass Surveillance. Retrieved from https://thedaywefightback.org/

The Economist. (2017, May 6). The world's most valuable resource is no longer oil, but data. Retrieved from https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

The Guardian. (2013, 9 Dec). Internet leaders speak out on the need for government reform of surveillance. Retrieved from https://www.theguardian.com/world/gallery/2013/dec/09/internet-leaders-speak-out-on-the-need-for-government-reform-of-surveillance

The New York Times Editorial Board. (2014, 17 Jan). The President on Mass Surveillance. Retrieved from http://www.nytimes.com/2014/01/18/opinion/the-president-on-mass-surveillance.html?_r=1

The Register. (2014, 23 Oct). Amazon's AWS opens data center in Germany – just as we said. Retrieved from http://www.theregister.co.uk/2014/10/23/aws_frankfurt_region/

Thibodeau, P. (2013). U.S. Cloud Vendors Face Backlash Over Prism. *Computerworld, 47*(14), 7.

Thomas, A. (2014, 18 Jan). Obama Promises Not to Spy on Merkel. Retrieved from http://www.wsj.com/news/articles/SB10001424052702304603704579329084011340404

Thomas, D., & Waters, R. (2014, 18 May). Cisco boss calls on Obama to rein in surveillance. Retrieved from http://on.ft.com/1nWFbn3

Thompson, A. G. (1996). Compliance with agreements in cross-cultural transactions: Some analytical issues. *Journal of international Business studies, 27*(2), 375-390.

Tibken, S. (2018, Apr 11). Questions to Mark Zuckerberg show many senators don't get Facebook. Retrieved from https://www.cnet.com/news/some-senators-in-congress-capitol-hill-just-dont-get-facebook-and-mark-zuckerberg/

Timberg, C. (2013, 6 Sep). Google encrypts data amid backlash against NSA spying. Retrieved from https://www.washingtonpost.com/business/technology/google-encrypts-data-amid-backlash-against-nsa-spying/2013/09/06/9acc3c20-1722-11e3-a2ec-b47e45e6f8ef_story.html

Timberg, C., & Nakashima, E. (2013, July 7). Agreements with private companies protect U.S. access to cables' data for surveillance. *The Washington Post.* Retrieved from http://www.washingtonpost.com/business/technology/agreements-with-private-companies-protect-us-access-to-cables-data-for-surveillance/2013/07/06/aa5d017a-df77-11e2-b2d4-ea6d8f477a01_story.html?hpid=z4

Ting-Toomey, S. (1991). Intimacy expressions in three cultures: France, Japan, and the United States. *International Journal of Intercultural Relations, 15*(1), 29-46.

Tinsley, C. (1998). Models of conflict resolution in Japanese, German, and American cultures. *Journal of Applied Psychology, 83*(2), 316.

TNW. (2016, Mar 11). Why AWS dominates the cloud services market. Retrieved from https://thenextweb.com/offers/2016/03/11/amazon-web-services-dominates-cloud-services-market/

Tomlinson, E. C., Dineen, B. R., & Lewicki, R. J. (2004). The road to reconciliation: Antecedents of victim willingness to reconcile following a broken promise. *Journal of Management, 30*(2), 165-187.

Traynor, I. (2013, July 4). European firms 'could quit US internet providers over NSA scandal'. *The Guardian.* Retrieved from http://www.guardian.co.uk/world/2013/jul/04/european-us-internet-providers-nsa

Tremblay, M. A. (1957). The Key Informant Technique: A Nonethnographic Application. *American Anthropologist, 59*(4), 688-701.

Triandis, H. C. (1972). The analysis of subjective culture.

Triandis, H. C. (2001). Individualism-collectivism and personality. *Journal of Personality, 69*(6), 907-924.

Triandis, H. C. (2018). *Individualism and collectivism*: Routledge.

Trigueros-Preciado, S., Pérez-González, D., & Solana-González, P. (2013). Cloud computing in industrial SMEs: identification of the barriers to its adoption and effects of its application. *Electronic Markets*, 1-10.

Trompenaars, F. (1993). *Riding the waves of culture: understanding cultural diversity in business*: Economist Books.

Twing-Kwong, S., Albaum, L. G., & Fullgrabe, L. (2013). Trust in customer-salesperson relationship in China's retail sector. *International Journal of Retail & Distribution Management, 41*(3), 226-248. doi:10.1108/09590551311306264

U.S. (1978). Foreign Intelligence Surveillance Act of 1978. *PUBLIC LAW 95-511.* Retrieved from http://www.gpo.gov/fdsys/pkg/STATUTE-92/pdf/STATUTE-92-Pg1783.pdf

U.S. (1986). Electronic Communications Privacy Act of 1986. *18 U.S.C. § 2510-22.* Retrieved from https://it.ojp.gov/default.aspx?area=privacy&page=1285

U.S. (2001). USA PATRIOT Act of 2001. *PUBLIC LAW 107-56.* Retrieved from http://www.fincen.gov/statutes_regs/patriot/

U.S. (2004). Intelligence Reform and Terrorism Prevention Act of 2004. *PUBLIC LAW 108-458.* Retrieved from https://www.archives.gov/files/declassification/pidb/legislation/pdfs/public-law-108-458.pdf

U.S. (2005). USA PATRIOT Improvement and Reauthorization Act. *H.R. 3199.* Retrieved from http://www.gpo.gov/fdsys/pkg/BILLS-109hr3199enr/pdf/BILLS-109hr3199enr.pdf

U.S. (2007). Protect America Act of 2007. *Public Law 110-55.* Retrieved from http://www.gpo.gov/fdsys/granule/STATUTE-121/STATUTE-121-Pg552/content-detail.html

U.S. (2008). FISA Amendments Act of 2008. *H.R. 6304.* Retrieved from https://www.govtrack.us/congress/bills/110/hr6304/text

U.S. (2011). PATRIOT Sunsets Extension Act. *PUBLIC LAW 112-14.* Retrieved from http://npl.ly.gov.tw/pdf/7500.pdf
U.S. (2012). FISA Amendments Act Reauthorization Act of 2012. *H.R. 5949.* Retrieved from https://www.govtrack.us/congress/bills/112/hr5949
U.S. (2015). USA FREEDOM Act of 2015. *H. R. 2048.* Retrieved from https://www.congress.gov/bill/114th-congress/house-bill/2048
U.S. (2018a). CLOUD Act. *H.R.4943.* Retrieved from https://www.congress.gov/bill/115th-congress/house-bill/4943
U.S. (2018b, Apr 11). Facebook, Social Media Privacy, and the Use and Abuse of Data. Retrieved from https://www.judiciary.senate.gov/meetings/facebook-social-media-privacy-and-the-use-and-abuse-of-data
Ullah, S., & Xuefeng, Z. (2013). Cloud Computing Research Challenges. *arXiv preprint arXiv:1304.3203*.
UN. (2013, December 19). General Assembly backs right to privacy in digital age. *United Nations.* Retrieved from http://www.un.org/apps/news/story.asp?NewsID=46780
United Nations. (1948). The Universal Declaration of Human Rights Retrieved from http://www.un.org/en/documents/udhr/
USAID. (1996). Conducting Key Informant Interviews: Performance Monitoring & Evaluation TIPS. *Center for Development Information and Evaluation*. Retrieved from http://pdf.usaid.gov/pdf_docs/PNABS541.pdf
Uslaner, E. M. (2002). *The moral foundations of trust*: Cambridge University Press.
Uusitalo, I., Karppinen, K., Juhola, A., & Savola, R. (2010, Nov. 30 2010-Dec. 3 2010). *Trust and Cloud Services - An Interview Study.* Paper presented at the Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on.
Vacca, J. R. (2016). *Cloud Computing Security: Foundations and Challenges*: CRC Press.
Vaid, K. (2016, October 31). Microsoft reimagines open source cloud hardware. Retrieved from https://azure.microsoft.com/en-us/blog/microsoft-reimagines-open-source-cloud-hardware/
Van den Broeck, E., Poels, K., & Walrave, M. (2015). Older and wiser? Facebook use, privacy concern, and privacy protection in the life stages of emerging, young, and middle adulthood. *Social Media+ Society, 1*(2), 2056305115616149.
Van der Aalst, W. M. (2014). Data scientist: The engineer of the future *Enterprise interoperability VI* (pp. 13-26): Springer.
Van Hoboken, J., Arnbak, A., & Van Eijk, N. (2012). Cloud Computing in Higher Education and Research Institutions and the USA Patriot Act. *Available at SSRN 2181534*.
van Teijlingen, E., & Vanora, H. (2002). The importance of pilot studies. *Nursing Standard, 16*(40), 33-36.
Vaquero, L. M., Rodero-Merino, L., Caceres, J., & Lindner, M. (2008). A break in the clouds: towards a cloud definition. *SIGCOMM Comput. Commun. Rev., 39*(1), 50-55. doi:10.1145/1496091.1496100
Varalakshmi, P., & Judgi, T. (2016). Multifaceted trust management framework based on a trust level agreement in a collaborative cloud. *Computers & Electrical Engineering*. doi:10.1016/j.compeleceng.2016.10.002
Varia, J. (2008). Cloud Architectures. *Amazon Web Services, Inc. .* Retrieved from http://media.amazonwebservices.com/AWS_Cloud_Architectures.pdf
Venters, W., & Whitley, E. A. (2012). A critical review of cloud computing: researching desires and realities. *Journal of Information Technology, 27*(3), 179-197.
Vidal, J., & Goldenberg, S. (2014, January 30). Snowden revelations of NSA spying on Copenhagen climate talks spark anger. Retrieved from https://www.theguardian.com/environment/2014/jan/30/snowden-nsa-spying-copenhagen-climate-talks

VMware. (2015, March 16). vCloud Air comes to Germany…and beyond. Retrieved from http://vmwareemeablog.com/uk/vcloud-air-comes-to-germanyand-beyond/?src=vcld-2015-1-blog-emeagermanyannouncement-o-in-1966

Voigt, P., & von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide*: Springer International Publishing.

Volmer, H. (2013, November 6). Freie Fahrt für freie Daten [Free travel for free data]. Retrieved from http://www.n-tv.de/politik/Freie-Fahrt-fuer-freie-Daten-article11679526.html

Volz, D. (2016, September 2). Microsoft gets support in gag order lawsuit from U.S. companies. Retrieved from http://www.reuters.com/article/us-usa-microsoft-privacy-idUSKCN1182SY

Vosselman, E., & Van der Meer-Kooistra, J. (2009). Accounting for control and trust building in interfirm transactional relationships. *Accounting, Organizations and Society, 34*(2), 267-283.

VZBV. (2018, 14 Feb). Facebook in breach of German data protection law. Retrieved from https://www.vzbv.de/sites/default/files/downloads/2018/02/14/18-02-12_vzbv_pm_facebook-urteil_en.pdf

Walden, I. (2012). Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent. In S. Pearson & G. Yee (Eds.), *Privacy and Security for Cloud Computing*. London: Springer.

Walterbusch, M., Fietz, A., & Teuteberg, F. (2017). Missing cloud security awareness: investigating risk exposure in shadow IT. *Journal of Enterprise Information Management, 30*(4), 644-665.

Wang, L., Ranjan, R., Chen, J., & Benatallah, B. (2017). *Cloud Computing: Methodology, Systems, and Applications*: CRC Press.

Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review, 4*(5), 193-220. doi:10.2307/1321160

Warrington, T. B., Abgrab, N. j., & Caldwell, H. M. (2000). Building trust to develop competitive advantage in e-business relationships. *Competitiveness Review, 10*(2), 160-168.

Waters, R. (2016, May 4). Artificial intelligence in the cloud promises to be the next great disrupter. Retrieved from https://www.ft.com/content/106ada72-ef52-11e5-9f20-c3a047354386

Weber, M. (1968). On Charisma and Institution Building. In S. N. Eisenstadt (Ed.): University of Chicago Press.

Weinhardt, C., Anandasivam, A., Blau, B., Borissov, N., Meinl, T., Michalk, W., & Stößer, J. (2009). Cloud computing–a classification, business models, and research directions. *Business & Information Systems Engineering, 1*(5), 391-399.

Weitz, B. A., Sujan, H., & Sujan, M. (1986). Knowledge, motivation, and adaptive behavior: A framework for improving selling effectiveness. *Journal of Marketing, 50*(4), 174-191.

Westin, A. F. (1967). *Privacy and Freedom*. New York: Atheneum.

Whitener, E. M., Brodt, S. E., Korsgaard, M. A., & Jon, M. W. (1998). Managers as Initiators of Trust: An Exchange Relationship Framework for Understanding Managerial Trustworthy Behavior. *The Academy of Management Review, 23*(3), 513-530. doi:10.2307/259292

Whittaker, Z. (2011a, April 26). Case study: How the USA PATRIOT Act can be used to access EU data [Web log post]. *ZDNet*. Retrieved from http://www.zdnet.com/blog/igeneration/case-study-how-the-usa-patriot-act-can-be-used-to-access-eu-data/8805

Whittaker, Z. (2011b, July 5). EU demands answers over Microsoft's Patriot Act admission [Web log post]. *ZDNet*. Retrieved from http://www.zdnet.com/blog/igeneration/eu-demands-answers-over-microsofts-patriot-act-admission/11290

Whittaker, Z. (2011c, June 28). Microsoft admits Patriot Act can access EU-based cloud data [Web log post]. *ZDNet*. Retrieved from http://www.zdnet.com/blog/igeneration/microsoft-admits-patriot-act-can-access-eu-based-cloud-data/11225

Whittaker, Z. (2011d, April 25). USA PATRIOT Act and the controversy of Canada. Retrieved from http://www.zdnet.com/article/usa-patriot-act-and-the-controversy-of-canada/

Whittaker, Z. (2012, December 4). Patriot Act can "obtain" data in Europe, researchers say. *CBS News.* Retrieved from http://www.cbsnews.com/news/patriot-act-can-obtain-data-in-europe-researchers-say/

Wholey, D. R., & Brittain, J. (1989). Characterizing environmental variation. *Academy of management journal, 32*(4), 867-882.

Willcocks, L. P., Sauer, C., & Lacity, M. C. (2016). *Enacting Research Methods in Information Systems*: Springer International Publishing.

Williamson, O. E. (1979). Transaction-cost economics: the governance of contractual relations. *JL & Econ., 22*, 233.

Williamson, O. E. (1993). Calculativeness, trust, and economic organization. *JL & Econ., 36*, 453.

Wilson, D. T. (1995). An Integrated Model of Buyer-Seller Relationships. *Journal of the Academy of Marketing Science, 23*(4), 335-345.

Wingfield, N., & Kang, C. (2016, July 14). Microsoft Wins Appeal on Overseas Data Searches. Retrieved from http://www.nytimes.com/2016/07/15/technology/microsoft-wins-appeal-on-overseas-data-searches.html?_r=0

Wolcott, H. F. (2008). *Ethnography: A Way of Seeing*: AltaMira Press.

Wong, A., & Sohal, A. (2002). An examination of the relationship between trust, commitment and relationship quality. *International Journal of Retail & Distribution Management, 30*(1), 34-50.

Wong, K. C. (2006). The USA PATRIOT Act: Some unanswered questions. *International Journal of the Sociology of Law, 34*(1), 1-41. doi:10.1016/j.ijsl.2005.12.001

Wood, J. A., Boles, J. S., Johnston, W., & Bellenger, D. (2008). Buyers' Trust of the Salesperson: An Item-Level Meta-Analysis. *The Journal of Personal Selling and Sales Management, 28*(3), 263-283.

Woolthuis, R. K., Hillebrand, B., & Nooteboom, B. (2005). Trust, Contract and Relationship Development. *Organization Studies, 26*(6), 813-840. doi:10.1177/0170840605054594

Wright, A., & Ehnert, I. (2010). Making sense of trust across cultural contexts. In M. N. K. Saunders, D. Skinner, G. Dietz, N. Gillespie, & R. J. Lewicki (Eds.), *Organizational trust: A cultural perspective* (pp. 107-126).

Xu, J. D., Cenfetelli, R. T., & Aquino, K. (2016). Do different kinds of trust matter? An examination of the three trusting beliefs on satisfaction and purchase behavior in the buyer–seller context. *The Journal of Strategic Information Systems, 25*(1), 15-31.

Yamagishi, T., & Yamagishi, M. (1994). Trust and commitment in the United States and Japan. *Motivation and emotion, 18*(2), 129-166.

Yang, D.-J., & Wu, M. J. (2014). Does Customer Trust Play a Mediating Role Between Salesperson Competence and Performance? *International Journal of Management, Economics and Social Sciences, 3*(2), 100-121.

Yang, H., & Tate, M. (2009). *Where are we at with cloud computing?: a descriptive literature review.* Paper presented at the 20th Australasian Conference on Information Systems, Melbourne.

Yang, H., & Tate, M. (2012). A descriptive literature review and classification of cloud computing research. *CAIS, 31*, 2.

Yao-Hua Tan, W. T. (2000). Toward a generic model of trust for electronic commerce. *International Journal of Electronic Commerce, 5*(2), 61-74.

Yin, R. K. (2009). *Case study research: design and methods*: Sage Publications.

Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *Journal of Consumer affairs, 43*(3), 389-418.

Young-Ybarra, C., & Wiersema, M. (1999). Strategic Flexibility in Information Technology Alliances: The Influence of Transaction Cost Economics and Social Exchange Theory. *Organization Science, 10*(4), 439-459. doi:10.2307/2640365

Young, L., & Albaum, G. (2003). Measurement of Trust in Salesperson-Customer Relationships in Direct Selling. *The Journal of Personal Selling and Sales Management, 23*(3), 253-269.

Young, L., & Wilkinson, I. F. (1989). The role of trust and co-operation in marketing channels: a preliminary study. *European Journal of Marketing, 23*(2), 109-122.

Yousfi, H. (2010). Culture and trust in contractual relationships: a French-Lebanese cooperation. In M. N. K. Saunders, D. Skinner, G. Dietz, N. Gillespie, & R. J. Lewicki (Eds.), *Organizational trust: A cultural perspective* (pp. 227).

Zacharakis, Z. (2013, July 4). Vorsprung durch Spionage [Advantage through espionage]. Retrieved from http://www.zeit.de/wirtschaft/2013-07/wirtschaftsspionage-nsa-usa-deutschland

Zaheer, A., McEvily, B., & Perrone, V. (1998). Does Trust Matter? Exploring the Effects of Interorganizational and Interpersonal Trust on Performance. *Organization Science, 9*(2), 141-159. doi:10.2307/2640350

Zaheer, S., & Zaheer, A. (2006). Trust across borders. *Journal of international Business studies, 37*(1), 21-29.

Zak, P. J., & Knack, S. (2001). Trust and growth. *The economic journal, 111*(470), 295-321.

Zaltman, G., & Moorman, C. (1988). The importance of personal trust in the use of research. *Journal of Advertising Research, 28*(5), 16-24.

Zand, D. E. (1972). Trust and managerial problem solving. *Administrative science quarterly*, 229-239.

Zaske, S. (2015, October 26). While US and UK governments oppose encryption, Germany promotes it. Why? Retrieved from http://www.zdnet.com/article/while-us-and-uk-govts-oppose-encryption-germany-promotes-it-why/

ZDF. (2014, January 18). Interview US-President Barack Obama – Claus Kleber. Retrieved from http://www.heute.de/ZDF/zdfportal/blob/31540850/1/data.pdf

Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: state-of-the-art and research challenges. *Journal of Internet Services and Applications, 1*(1), 7-18.

Zhao, Y., & Tamer Cavusgil, S. (2006). The effect of supplier's market orientation on manufacturer's trust. *Industrial Marketing Management, 35*(4), 405-414. doi:10.1016/j.indmarman.2005.04.001

Zhu, B., Habisch, A., & Thøgersen, J. (2018). The Importance Of Cultural Values And Trust For Innovation—A European Study. *International Journal of Innovation Management, 22*(02), 1850017.

Zucker, L. G. (1986). Production of trust: Institutional sources of economic structure, 1840–1920. *Research in Organizational Behavior, 8*, 53-111.

Appendix 1: “Interview questions”

The following tables list the pool of questions for the German companies and the local sales representatives of the U.S. cloud providers. The questions market with “Pilot” were already part of the first pilot interview, the questions marked as “New” were added in the course of the following interviews.

Interview questions for German companies

No.	Objective	English	German	Context	Version
G1	General/ introduction	Can you please give me a brief introduction to your company and the IT department?	Können Sie mir bitte eine kurze Einführung in Ihre Firma und die IT-Abteilung geben?	General background about the company and IT department.	Pilot
G2	General/ introduction	How would you describe your role in your organisation?	Wie würden Sie Ihre Rolle in Ihrem Unternehmen beschreiben?	General information about the interviewee.	Pilot
G3	General/ introduction	What is your company’s experiences with cloud computing and more particularly with public cloud services?	Welche Erfahrungen hat Ihr Unternehmen bisher mit Cloud Computing und insbesondere mit Public Cloud-Diensten gesammelt?	Company history and experience with cloud computing.	Pilot
I1	RO1 Importance of trust	How important is the concept of trust for using public cloud services for your company?	Wie wichtig ist Ihrem Unternehmen das Thema Vertrauen für die Verwendung von Public Cloud-Diensten?	Research question on how important trust is for cloud computing adoption.	Pilot
I2	RO1 Importance of trust	How would you assess the influence of the German culture and history on the perception of the revelations by Edward Snowden?	Wie würden Sie den Einfluss der deutschen Kultur und Geschichte auf die Sichtweise auf die Enthüllungen durch Edward Snowden beurteilen?	Question on the cultural and historical aspects of the topic.	New
I3	RO1 Importance of trust	How much influence does the sector or industry a company is operating in have on the adoption of public cloud computing services?	Welche Rolle spielt Ihrer Meinung nach die Branche in der sich ein Unternehmen befindet bei der Verwendung von Public Cloud-Diensten?	Question on influence of the sector.	New
P1	RO2a Product trust	What do you think about the overall features, performance and quality of U.S. public cloud services?	Wie beurteilen Sie insgesamt die Funktionalitäten, Qualität und Leistungsfähigkeit	Question if “the product/service will fulfil its functions as	Pilot

			von US-Public Cloud-Diensten?	understood by the buyer.”	
P2	RO2a Product trust	How do you think about the features, performance and quality of U.S. public cloud services in comparison to cloud services from Germany or other countries in the EU?	Wie schätzen Sie die Funktionalitäten, Qualität und Leistungsfähigkeit von US-Public Cloud-Diensten im Vergleich zu Cloud-Diensten aus Deutschland oder anderen Ländern der EU ein?	Product trust in U.S. public cloud services in comparison to cloud services from other countries.	Pilot
S1	RO2c Salesperson trust	How important is a trustful relationship with the local salespeople of your suppliers/providers to you?	Wie wichtig ist Ihnen ein vertrauensvolles Verhältnis zu den lokalen Vertriebsmitarbeitern Ihrer Zulieferer/Lieferanten?	General importance of a trustful relationship with suppliers/providers.	Pilot
S2	RO2c Salesperson trust	How much do you trust the statements and promises of the local salespeople of the U.S. public cloud providers?	In wieweit vertrauen Sie den Aussagen und Versprechen der lokalen Vertriebsmitarbeiter der US- Public Cloud-Anbieter?	Trust in what the local salesperson is communicating to the German companies.	Pilot
C1	RO2b Company trust	How would you describe your trust relationship to U.S. public cloud computing service providers?	Wie würden Sie Ihr Vertrauensverhältnis zu US- Public Cloud-Anbietern beschreiben?	General description of the trust of the German company in the U.S. public cloud providers.	Pilot
C2	RO2b Company trust	How would you, in contrast, assess your trust in public cloud providers based in Germany or other countries in the EU?	Wie beurteilen Sie im Gegensatz dazu Ihr Vertrauen in Public Cloud-Anbieter mit Unternehmenssitz in Deutschland oder anderen Ländern der EU?	Company trust comparison between U.S. providers and companies based in Germany/EU.	Pilot
L1	RO2c Foreign government trust	What influence do U.S. legislation and government agency access have on your trust in U.S. public cloud services, the local salespeople and the U.S. provider company?	Welchen Einfluss haben die US-Gesetzgebung und Zugriffsmöglichkeiten der Regierungsorganisationen auf Ihr Vertrauen in US-Public Cloud-Dienste, die lokalen Vertriebsmitarbeiter und die US-Public Cloud-Anbieter?	Impact of U.S. legislation and government agencies on those trust relationships.	Pilot

L2	RO2c Foreign government trust	To what extend have the disclosure and discussions regarding the NSA PRISM programme and the USA PATRIOT Act changed your trust relationship with U.S. public cloud computing services?	Inwieweit haben die Enthüllungen und Diskussionen bezüglich des NSA PRISM-Programms und des USA PATRIOT Act Ihr Vertrauensverhältnis zu US-Public Cloud-Diensten verändert?	Influence of the NSA revelations on the trust relationship.	Pilot
L3	RO2c Foreign government trust	How would you in particular assess the risks of economic espionage by using U.S. public cloud services?	Wie würden Sie insbesondere die Gefahr der Wirtschaftsspionage durch den Einsatz von US-Public Cloud-Diensten beurteilen?	Distinct focus on economic espionage by using U.S. public cloud services.	New
I1	RO3 How to improve trust	What do you think U.S. public cloud providers could do to improve the trust German companies have in their cloud services?	Was müssten US-Public Cloud-Anbieter aus Ihrer Sicht tun, um das Vertrauen deutscher Unternehmen in Ihre Cloud-Dienste zu verbessern?	Identify ways that U.S. public cloud providers can improve the trust German companies have in their services.	Pilot
I2	RO3 How to improve trust	What changes need to be made to U.S. legislation and government agency access so that you can trust U.S. public cloud services as much as cloud services from Germany or other countries in the EU?	Welche Änderungen müssten an der US-Gesetzgebung und Zugriffsmöglichkeiten der Regierungsorganisationen vorgenommen werden, damit Sie dasselbe Vertrauen in US-Public Cloud-Dienste haben wie in Cloud-Dienste aus Deutschland oder anderen Ländern der EU?	How to improve trust by changing U.S. legislation and government agency access.	Pilot
I3	RO3 How to improve trust	Is there anything the German government or the EU could do to improve your trust in U.S. public cloud services?	Was könnte die deutsche Regierung oder die EU Ihrer Meinung nach tun um Ihr Vertrauen in US-Public Cloud-Dienste zu verbessern?	What the German government or the EU could do to improve trust.	Pilot
G4	General/ introduction	Is there anything that I might have forgotten to ask or anything that you would like to add?	Gibt es aus Ihrer Sicht etwas das ich vergessen habe zu fragen oder was Sie gerne noch ergänzen möchten?	General question to make sure that the participants had the chance to add further insights.	Pilot

Interview questions for U.S. cloud providers

No.	Objective	English	German	Context
G1	General/ introduction	Can you please give me a brief introduction to your company and the department you work in?	Können Sie mir bitte eine kurze Einführung in Ihre Firma und die Abteilung geben in der Sie arbeiten?	General background about the U.S. cloud provider
G2	General/ introduction	How would you describe your role in your organisation?	Wie würden Sie Ihre Rolle in Ihrem Unternehmen beschreiben?	General information about the interviewee.
G3	General/ introduction	What cloud products are you offering to the German market?	Welche Cloud-Produkte bieten Sie auf dem deutschen Markt an?	Company history and experience with cloud computing.
I1	RO1 Importance of trust	How important is the concept of trust for using public cloud services for your customers?	Wie wichtig ist Ihren Kunden das Thema Vertrauen für die Verwendung von Public Cloud-Diensten?	Research question on how important trust is for cloud computing adoption.
I2	RO1 Importance of trust	How would you assess the influence of the German culture and history on the perception of the revelations by Edward Snowden?	Wie würden Sie den Einfluss der deutschen Kultur und Geschichte auf die Sichtweise auf die Enthüllungen durch Edward Snowden beurteilen?	Question on the cultural and historical aspects of the topic.
I3	RO1 Importance of trust	How much influence does the sector or industry a company is operating in have on the adoption of public cloud computing services?	Welche Rolle spielt Ihrer Meinung nach die Branche in der sich ein Unternehmen befindet bei der Verwendung von Public Cloud-Diensten?	Question on influence of the sector.
P1	RO2a Product trust	What do your customers think about the overall features, performance and quality of U.S. public cloud services?	Wie beurteilen Ihre Kunden insgesamt die Funktionalitäten, Qualität und Leistungsfähigkeit von US-Public Cloud-Diensten?	Question if “the product/service will fulfil its functions as understood by the buyer.”
P2	RO2a Product trust	How do your customers think about the features, performance and quality of U.S. public cloud services in comparison to cloud services from Germany or other countries in the EU?	Wie schätzen Ihre Kunden die Funktionalitäten, Qualität und Leistungsfähigkeit von US-Public Cloud-Diensten im Vergleich zu Cloud-Diensten aus Deutschland oder anderen Ländern der EU ein?	Product trust in U.S. public cloud services in comparison to cloud services from other countries.
S1	RO2c Salesperso n trust	How important is a trustful relationship with the local salespeople of your company for your customers?	Wie wichtig ist Ihren Kunden ein vertrauensvolles Verhältnis zu den lokalen Vertriebsmitarbeitern Ihres Unternehmens?	General importance of a trustful relationship with suppliers/providers.
S2	RO2c Salesperso n trust	How much do your customers trust the statements and promises of the local salespeople of your company?	In wieweit vertrauen Ihre Kunden den Aussagen und Versprechen der lokalen Vertriebsmitarbeiter Ihres Unternehmens?	Trust in what the local salesperson is communicating to the German companies.
C1	RO2b Company trust	How would you describe the trust of your customers in U.S. public	Wie würden Sie das Vertrauensverhältnis Ihrer Kunden zu US- Public Cloud-	General description of the trust of the German company

		cloud computing service providers like you?	Anbietern wie Ihnen beschreiben?	in the U.S. public cloud providers.
C2	RO2b Company trust	How would you, in contrast, assess the trust of your customers in public cloud providers based in Germany or other countries in the EU?	Wie beurteilen Sie im Gegensatz dazu das Vertrauensverhältnis Ihrer Kunden in Public Cloud-Anbieter mit Unternehmenssitz in Deutschland oder anderen Ländern der EU?	Company trust comparison between U.S. providers and companies based in Germany/EU.
L1	RO2c Foreign government trust	What influence do U.S. legislation and government agency access have for your customers on their trust in U.S. public cloud services, the local salespeople and the U.S. provider company?	Welchen Einfluss haben die US-Gesetzgebung und Zugriffsmöglichkeiten der Regierungsorganisationen auf das Vertrauen Ihrer Kunden in US-Public Cloud-Dienste, die lokalen Vertriebsmitarbeiter und die US-Public Cloud-Anbieter?	Impact of U.S. legislation and government agencies on those trust relationships.
L2	RO2c Foreign government trust	To what extend have the disclosure and discussions regarding the NSA PRISM programme and the USA PATRIOT Act changed the trust of your customers in U.S. public cloud computing services?	Inwieweit haben die Enthüllungen und Diskussionen bezüglich des NSA PRISM-Programms und des USA PATRIOT Act das Vertrauensverhältnis Ihrer Kunden zu US-Public Cloud-Diensten verändert?	Influence of the NSA revelations on the trust relationship.
L3	RO3 How to improve trust	How do your customers in particular assess the risks of economic espionage by using U.S. public cloud services?	Wie beurteilen Ihre Kunden insbesondere die Gefahr der Wirtschaftsspionage durch den Einsatz von US-Public Cloud-Diensten?	Distinct focus on economic espionage by using U.S. public cloud services.
I1	RO3 How to improve trust	What do your customers think that U.S. public cloud providers could do to improve the trust German companies have in your cloud services?	Was müssten US-Public Cloud-Anbieter aus der Sicht Ihrer Kunden tun, um das Vertrauen deutscher Unternehmen in Ihre Cloud-Dienste zu verbessern?	Identify ways that U.S. public cloud providers can improve the trust German companies have in their services.
I2	RO3 How to improve trust	What changes need to be made to U.S. legislation and government agency access so that your customers can trust U.S. public cloud services as much as cloud services from Germany or other countries in the EU?	Welche Änderungen müssten an der US-Gesetzgebung und Zugriffsmöglichkeiten der Regierungsorganisationen vorgenommen werden, damit Ihre Kunden dasselbe Vertrauen in US-Public Cloud-Dienste haben wie in Cloud-Dienste aus Deutschland oder anderen Ländern der EU?	How to improve trust by changing U.S. legislation and government agency access.
I3	General/ introduction	Is there anything the German government or the EU could do to improve the trust of your customers in U.S. public cloud services?	Was könnte die deutsche Regierung oder die EU Ihrer Meinung nach tun, um das Vertrauen Ihrer Kunden in US-Public Cloud-Dienste zu verbessern?	What the German government or the EU could do to improve trust.

G4	RO2c Foreign government trust	Is there anything that I might have forgotten to ask or anything that you would like to add?	Gibt es aus Ihrer Sicht etwas das ich vergessen habe zu fragen oder was Sie gerne noch ergänzen möchten?	General question to make sure that the participants had the chance to add further insights.

Appendix 2: “Participant recruitment”

Social network cover letter

The following message was sent out to potential interview candidates identified on the professional social networks XING and LinkedIn.

Das Vertrauensverhältnis von deutschen Unternehmen in US Cloud-Anbieter	**The trust of German companies in U.S. cloud providers**
Sehr geehrte/r Frau/Herr _____,	Dear _____,
mein Name ist Sven Gerritsen und ich schreibe derzeit an meiner Doktorarbeit an der University of Gloucestershire in Kooperation mit der Fachhochschule des Mittelstands.	My name is Sven Gerritsen and I am currently working on my doctoral thesis at the University of Gloucestershire in cooperation with the Fachhochschule des Mittelstands.
Das Thema meiner Arbeit ist das Vertrauensverhältnis von deutschen Unternehmen in US-amerikanische Public Cloud-Anbieter, insbesondere vor dem Hintergrund des USA PATRIOT Act und der NSA PRISM-Diskussionen.	The topic of my thesis is the trust of German companies in U.S. public cloud computing providers, particularly in the light of the USA PATRIOT Act and the NSA PRISM discussions.
Ich würde mich sehr darüber freuen, wenn ich zu diesem Thema ein Tiefeninterview mit Ihnen durchführen dürfte. Das Gespräch wird schätzungsweise eine Stunde dauern und an einem von Ihnen bevorzugten Ort oder telefonisch stattfinden.	I would be very happy if I could carry out a depth interview with you on this subject. The conversation will take about an hour and take place at a place of your choice or by telephone.
Meine Arbeit steht in keinerlei Zusammenhang zu meinem derzeitigen Arbeitgeber und ist vollständig selbstfinanziert. Die Namen aller beteiligten Personen und Firmen werden anonymisiert und gemäß den Richtlinien des „Handbook of Research Ethics“ der University of Gloucestershire durchgeführt.	My work is not related with my current employer and is completely self-financed. The names of all persons and companies involved will be anonymised and the research will be carried out according to the guidelines of the "Handbook of Research Ethics" of the University of Gloucestershire.
Ich freue mich über Ihre Rückmeldung, auch wenn diese negativ ausfallen sollte!	I am looking forward to your answer, even if this should turn out to be negative!
Mit den besten Grüßen,	With best regards,
Sven Gerritsen	Sven Gerritsen

Personal contacts cover letter

The following letter was sent to potential interview candidates recommended by friends, colleagues and acquaintances.

Das Vertrauensverhältnis von deutschen Unternehmen in US Cloud-Anbieter	**The trust of German companies in U.S. cloud providers**
Sehr geehrte/r Herr/Frau _____, mein Name ist Sven Gerritsen und ich schreibe derzeit an meiner Doktorarbeit an der University of Gloucestershire in England. Das Thema meiner Arbeit ist das Vertrauensverhältnis deutscher Unternehmen in US-amerikanische Public Cloud-Anbieter, insbesondere vor dem Hintergrund der NSA- und USA PATRIOT Act-Diskussionen. Sie wurden mir von _____ als fachkundiger und besonders geeigneter Gesprächspartner empfohlen, und ich würde mich daher sehr darüber freuen, wenn ich zu diesem Thema ein Interview mit Ihnen durchführen dürfte. Meine Arbeit ist vollständig selbstfinanziert und steht in keinerlei Zusammenhang zu meinem Arbeitgeber. Das Interview wird gemäß den Richtlinien des „Handbook of Research Ethics“ der Universität durchgeführt, wonach die Namen aller genannten Personen und Firmen anonymisiert werden. Ich werde mich in den nächsten Tagen telefonisch bei Ihnen melden, um Ihnen eventuelle Detailfragen zu beantworten, und einen möglichen Termin mit Ihnen abzustimmen. Mit den besten Grüßen, Sven Gerritsen	Dear _____, My name is Sven Gerritsen and I am currently working on my doctoral thesis at the University of Gloucestershire in England. The topic of my thesis is the trust of German companies in U.S. public cloud computing providers, particularly in the light of the NSA and USA PATRIOT discussions. You were recommended to me by _____ as an expert and particularly suitable interlocutor, and I would therefore be very pleased if I could carry out an interview with you on this subject. My work is completely self-financed and has no connection with my employer. The interview is conducted according to the guidelines of the University's "Handbook of Research Ethics", meaning that the names of all persons and companies will be anonymised. I will contact you in the next few days by telephone to answer any questions you may have and to make an appointment with you. With best regards, Sven Gerritsen

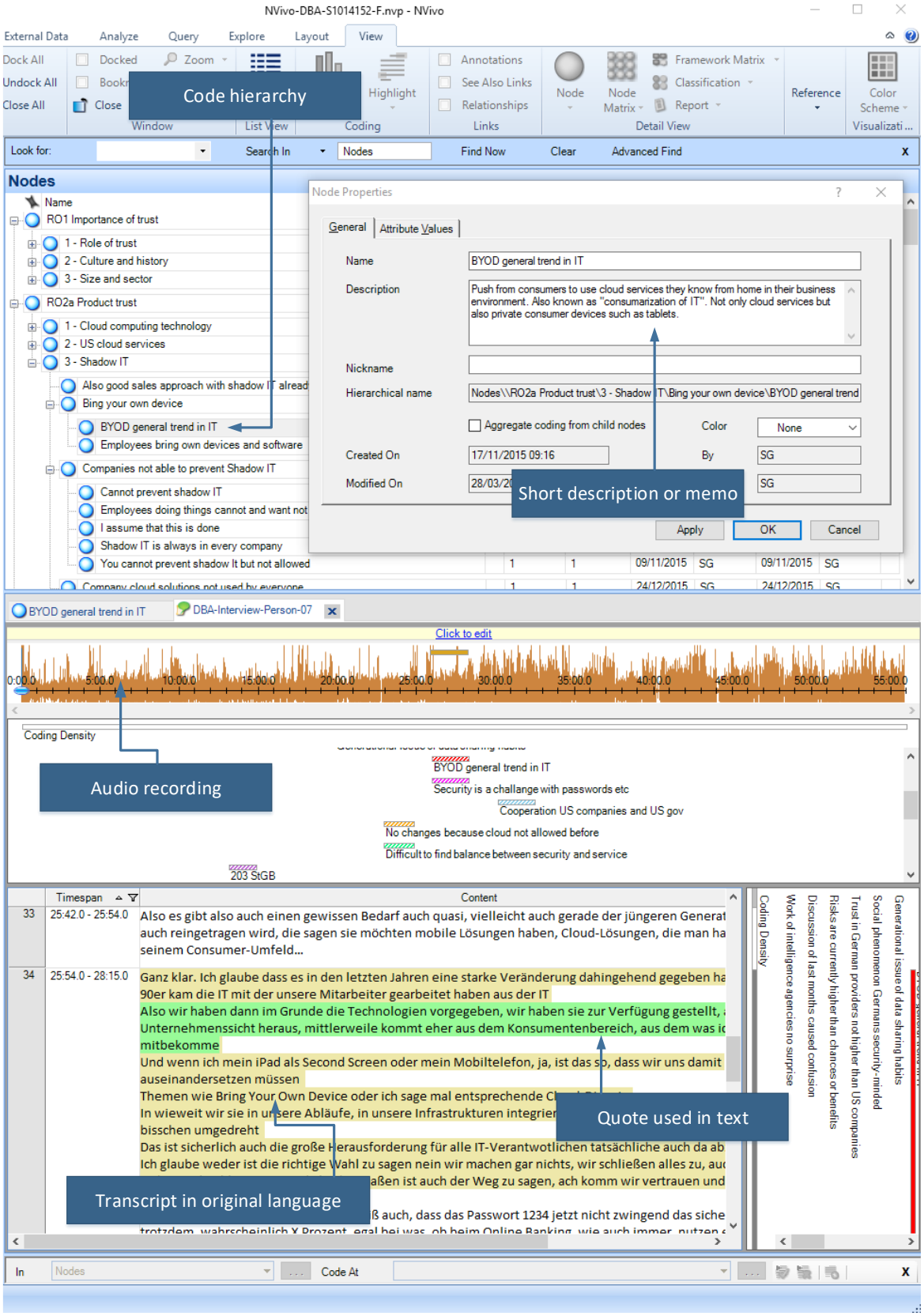
Phone call before interviews

The following list was used as a guide for calling the potential interviewees and to ask for permission to conduct an interview and schedule an appointment for the interview.

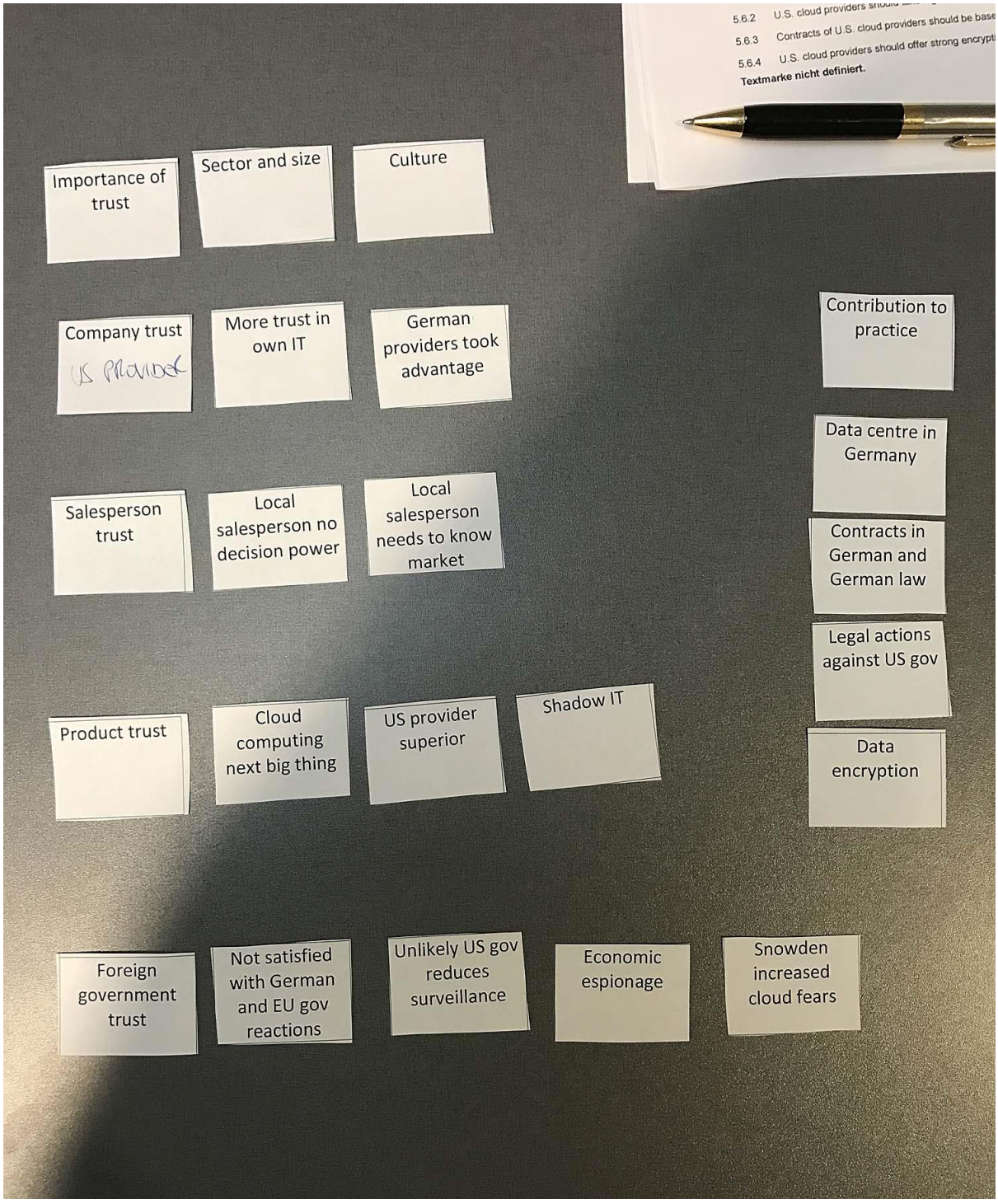
○ University of Gloucestershire in England ○ Vertrauensverhältnis deutscher Unternehmen in US-amerikanische Public Cloud-Anbieter ○ Hintergrund der NSA- und USA PATRIOT Act-Diskussionen ○ Das Interview besteht größtenteils aus offenen Fragen ○ Wird maximal eine Stunde dauern ○ Können Sie Aussagen zur IT- bzw. Cloud-Strategie machen? ○ Ich arbeite bei Microsoft Deutschland ○ Meine Arbeit steht in keinem Zusammenhang zu meinem Arbeitgeber ○ Vollständig selbstfinanziert ○ Gemäß den Richtlinien des „Handbook of Research Ethics“ der Universität durchgeführt ○ Anonymität aller Personen und Firmen sichergestellt ○ Ich würde das Gespräch gerne aufzeichnen ○ Erleichtert die spätere Auswertung ○ Aufzeichnungen bleiben vollständig bei mir ○ Termin im Monat X oder Y ○ Ich werde mich rechtzeitig vorher zwecks Terminfindung melden ○ Vielen Dank für Ihre Bereitschaft das Interview mit mir durchzuführen und ich freue mich auf unser Gespräch!	○ University of Gloucestershire in England ○ Trust relationship between German companies and U.S. public cloud providers ○ Background of the NSA and USA PATRIOT Act Discussions ○ The interview mainly consists of open questions ○ Will take maximum an hour ○ Can you make any comments on the IT or cloud strategy of your company? ○ I work for Microsoft Germany ○ My work is not related to my employer ○ Completely self-financed ○ According to the guidelines of the "Handbook of Research Ethics" of the university ○ Anonymity of all persons and company names ○ I would like to record our conversation ○ This helps with the subsequent evaluation ○ Recordings remain with me ○ Appointment in month X or Y ○ I will contact you again to fix a date ○ Thank you for your willingness to do the interview with me and I look forward to our conversation!

Appendix 3: “Coding and notes writing”

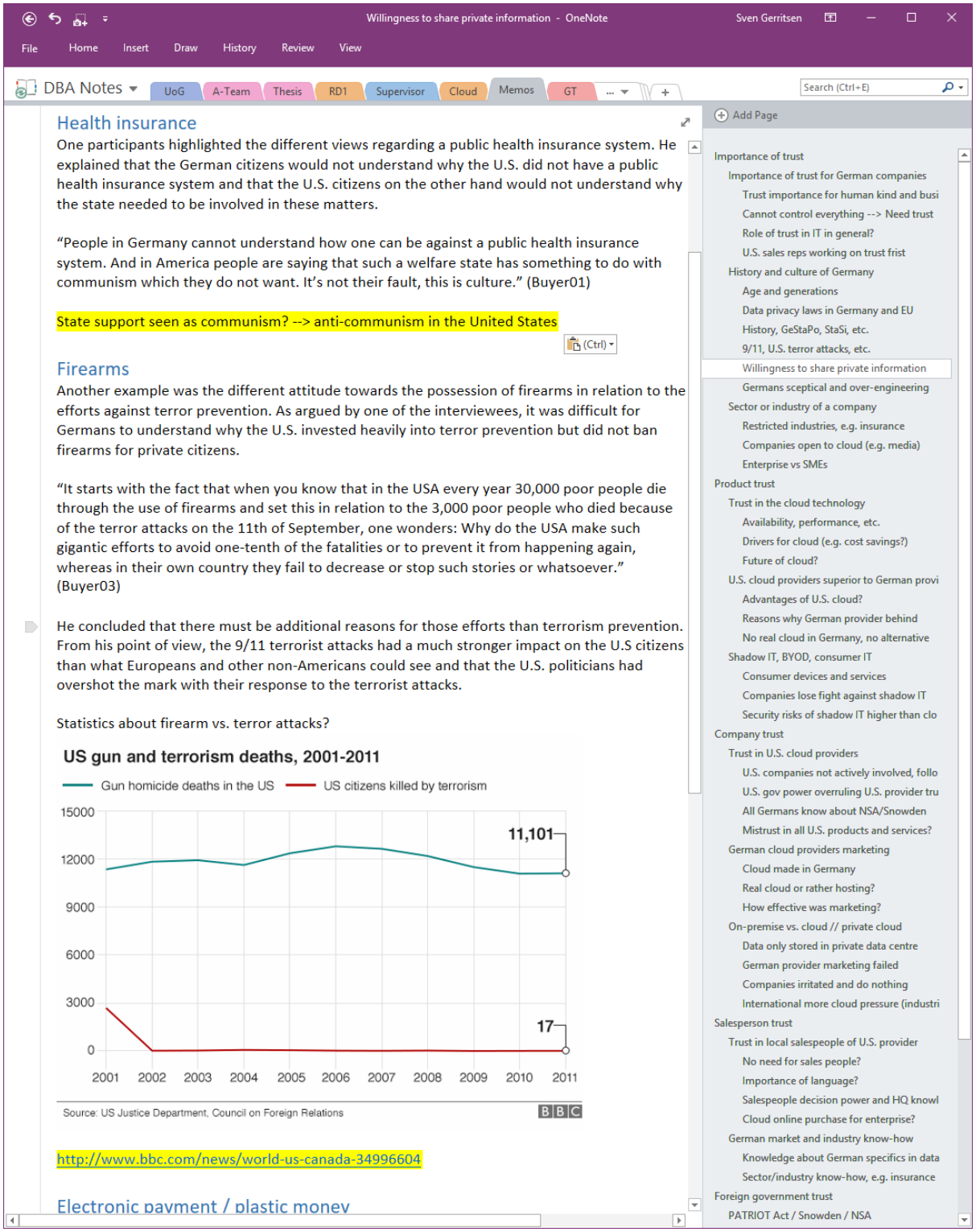
Example of coding in Nvivo for Windows.



Development of themes for the current research.



Example of notes written with Microsoft Office OneNote for Windows.



Appendix 4: “Additional quotes”

Importance of trust

Interviewee	Quote
Buyer01	“Trust is a matter of how well you know each other, how intensively you have already worked together. Trust needs to grow.”
Buyer03	„Yes, it is actually the deciding factor. If I wanted to try to make an IT system watertight to make sure that nobody can come in from the left or the right side, it is virtually impossible. We can set the hurdle or the bar as high as possible, but in the end, I have to find a partner whom I can trust. And this trust has been impaired by the American providers.”
Buyer04	“It plays a great role, an important role.”
Buyer06	“Building trust in something like that is not a matter of individual actions but rather takes several years. One can break that with a single stroke, rebuilding it will take years.”
Buyer08	“So, I think that trust is important for every human being. Everything is based on trust. It will not work if I can’t build that trust, no matter what business model I have, no matter what.”
Seller01	“Cloud is a trust business. You don’t sell with discounts but with trust.”
Seller04	“The topic is very important to me. The first two, three meetings are only geared to build trust.”
Seller05	“If there was a scale from 1-10 it would be 10.”
Seller05	“The biggest problem is when the IT guy says: No, I don’t trust you.”
Seller07	“Trust is the most critical point in building business relationships and came more and more in focus in the last years.”
Seller08	“Trust is one of the most important concepts in any kind of IT service. This is especially true for public cloud services. Public cloud trust is especially important.”

Cultural differences

Interviewee	Quote
Buyer01	“People in Germany cannot understand how one can be against a public health insurance system. And in America people are saying that such a welfare state has something to do with communism which they do not want. It’s not their fault, this is culture.”
Buyer01	“I have to admit that I cannot understand why the American people responded to 9/11 the way they did. Conversely, the Americans do not understand our reactions to our SS-time. Because there are simply cultural differences.”
Buyer01	“I do not know, from a cultural perspective, how you can easily bring together a Danish with an Italian.”
Buyer01	“It’s becoming more difficult. Even with European clouds.”
Buyer02	“It starts with the fact that American car dealers sometimes print their yearly salary on their business cards because they want to show how good they are. In Germany, you don’t even really talk to your best friends about your salary.”
Buyer02	“In this respect, it’s just like that it’s not about laws but about an entire data protection culture.”
Buyer03	“I believe that this is also a question of culture, starting with things such as a GeStaPo in the Third Reich or the StaSi in East Germany, where we already had such bugging operations and denunciation and eavesdropping operations. I think that, in consideration of those experiences, it is slightly more unpopular and unaccepted than it possibly is in the USA, where people didn’t make those experiences to this extend in the past.”
Buyer03	“It starts with the fact that when you know that in the USA every year 30,000 poor people die through the use of firearms and set this in relation to the 3,000 poor

	people who died because of the terror attacks on the 11th of September, one wonders: Why do the USA make such gigantic efforts to avoid one-tenth of the fatalities or to prevent it from happening again, whereas in their own country they fail to decrease or stop such stories or whatsoever."
Buyer03	"I recently had a telephone conversation with a colleague from the USA who told me that only during his visit in Germany some months ago he realised what a huge topic this is. He said: 'As an American I'm used to the fact that the government is looking over my shoulder. Do I like it? No, but as long as I do nothing wrong, I do not have a problem with it.' The mentality of the U.S. citizens is obviously a bit different."
Buyer06	"There is indeed a reason why we have one of the most sophisticated data privacy laws. This doesn't happen by chance but evolves from the culture of Germany."
Buyer06	"Germany is just very angular shaped, precise, delimited, organised. You don't have to find this beautiful, but it is like that."
Buyer07	"But I think that this is to some extent a social phenomenon. I believe that Germans are much more security-minded, perhaps because of the history, this is probably also a generational issue."
Buyer07	"So, my 19-year-old daughter has a completely different relationship to data and willingness to share data than basically… yes, let's say my generation, where you still consider carefully if you provide certain data, if you share them, that's what I think."
Buyer08	"So, from a cultural perspective, I would say, rather more cautious. Definitely because of the history that shaped us."
Buyer09	"There is a lot going on, and yet, we are in Germany, in my opinion, as usual, deliberately cautious. This has nothing to do with Mr Snowden."
Buyer09	"Not so much our neighbouring countries in Europe. But we are different from the Americans. And again, different from the Asians."
Buyer09	"Certainly because of how we are programmed by our family and schools. So, the ease with which Americans… the willingness to pay with plastic money came much later in Germany, maybe it did not even gain acceptance today."
Buyer10	"So, it is how you manage those different aspects in Germany is very much on the forefront of raising points to discuss around these things. So, I would agree that in my experience, probably German thinking is more advanced and more stringent around these areas than most other countries I would say, that I have come across."
Buyer10	"Yes, my observation, and this not a criticism or anything, my observation is that Germany is very sensitive around these matters of privacy, let's call it that, or all aspects of it."
Buyer10	"And that is something that, yeah, to your points, the U.S. companies struggle with a bit because their own landscape is so huge, you know. They wouldn't know where Morocco is or New Zealand or, you know, and therefore wouldn't think about as an impact on them."
Buyer11	"I think that Germany is very sophisticated in insuring that its citizens are protected. Very sophisticated as compared to other countries."
Buyer11	"The way things are set up, the structure… There is a structure to protect data privacy, to protect the individual."
Buyer11	"My wish would be to provide full disclosure. How are you storing my data, how are you handling my data? Full disclosure, transparency. Which is very important for Germany as a nation and for the German government. And the way of doing things is transparency. Culturally Germany demands a lot of transparency."
Buyer11	"I think in general the European countries have a stronger bias towards data privacy as an individual. I have learned that culturally there is a stronger tendency towards data privacy."
Buyer11	"I mean it is hard to undo 500 years, 800 years of culture. Yes, the Internet is a disrupter, yes cloud can be a disrupter, but I'm not going to undo 500 or 800 years."
Seller01	"The general German fear and scepticism. The Germans are always very sceptical. Germany always needs much longer. Disadvantages are always looked at first. The press always addresses fear. Germany is very conservative."
Seller01	"History plays an important role."
Seller02	"Why should I pay for an app?"

Seller03	“The Scandinavian markets are faster and more innovative.”
Seller03	“The discussions around the topic of personal data are also very emotional. The discussion can quickly become very unobjectively. It’s a cultural issue, the German is negative, cautious, Sir, I know something!”
Seller03	“The German history is not that long ago; younger people are just more open.”
Seller03	“Companies with younger employees are much easier. The younger people rather see the opportunities.”
Seller03	“The low-hanging fruits are customers with an international focus. Companies with a growth strategy and scalability requirements. Scalability is an important argument for the cloud.”
Seller04	“The German culture in terms of thoroughness… we want to be compliant… plays a vital role why the perception and understanding of risk are higher in Germany.”
Seller04	“We are the USA, we need to protect ourselves.”
Seller04	“This is again a cultural issue. We protect ourselves and if the Europeans don’t like it they need to do something about it themselves.”
Seller05	“Very high, I think. I believe that the topics around data protection and personal data rate high in Germany. Everyone is freaking out when there is a population census in Germany.”
Seller05	“If Germany wasn’t that big, U.S. cloud companies would not make such an effort to attend their special wishes.”
Seller05	“And that’s something we want to implement, or would like to implement, however, if this is coming is also depending on bodies such as the works council and others.”
Seller06	“Germans have a healthy suspicion about everything. With new technologies, they always say: Very well then, but…”
Seller06	“I believe that the cultural influence is very strong, I don’t have another explanation for it. A society which has been spied upon and which has been denounced over decades is much more sensitive to that.”
Seller06	“Today, the newer CIOs have a different view on these things.”
Seller06	“The difference to other countries is that there is a relatively high basic mistrustfulness in Germany.”
Seller06	“While the American engineer is looking for innovations, the German is already looking for the downsides”
Seller07	“Germans want to understand everything bit by bit before they take the first step in the cloud. Other countries get their experience by using the services and learn while they are using it.”
Seller07	“Especially international companies have a different focus.”
Seller07	“I would like to add that, from a technology perspective, companies in Germany already have a high IT standard, IT in enterprises relies on high standards. Therefore, the cloud is not as compelling as in other countries. German companies have many features already implemented in their own IT environment and many functionalities of the cloud are not required and could be covered with their own IT. This is an enormous difference to U.S. and East European countries.”
Seller08	“In my experience, in some EU countries, especially Scandinavia, UK and Ireland, the trust is from the start bigger and it is easier for U.S. cloud vendors. In Germany and France there is a historic distrust.”
Seller08	“It is more of an impression. I think but I don’t have a real proof for it, but I think that Germans are especially sensitive of giving away personal information because of the Nazi and communism history.”
Seller08	“Interestingly this it is not what customers tell me. They tell me that they cannot trust external companies with their data. It is more a gut feeling kind of argumentation by the customers. Those people are not convinced by facts. You have to change the gut-feelings of the companies.”

Sector

Interviewee	Quote
Buyer01	“This clearly means that the use of public cloud outside of Europe is almost impossible”
Buyer02	“It always depends very much on the industry”.
Buyer07	“I don’t know any insurance company that says confidently that they have everything somewhere in a cloud data centre.”
Buyer09	“The atmosphere is totally different from case to case. Everybody knows about the issue but approaches it differently.”
Buyer09	“Large enterprises like Daimler and Allianz insurance have much greater power. They can perhaps even have massive influence on developments.”
Buyer09	“In comparison with the really big companies it is very difficult for us. It is extremely difficult for us to influence anything, that’s the way it is”
Buyer10	“If we have a data breach, while it may be serious that there is a data breach, the consequences of that are less than perhaps other types of data breaches or other types of businesses.”
Buyer10	“It’s not good, because you don’t want any sort of breaches, but we are not in a business where information inherently can damage people.”
Seller07	“The size of a company has an influence on cloud adoption, especially if they are international.”
Seller08	“Let’s leave out the start-ups, because they couldn’t do their business without the public cloud. In large enterprises, there is not a substantial difference in the gut-feeling perspective. But in e.g. the financial or insurance industry there are regulations like §203 and they are very sensitive about that. But they are at the same time very open to legal arguments.”

Cloud computing technology

Interviewee	Quote
Buyer03	„It is certainly not an option for us to not do anything. Quite the contrary, we are even strongly pushing the cloud topic in the course of our IT infrastructure outsourcing. But as I said, we are paying a lot of attention to the question how the whole thing is realised.”
Buyer03	“As I said, the idea that I can use services on-demand, flexible, that I don’t have to make any investments, that I just have OPEX current expenses, that I can participate in the latest technical advances.”
Buyer05	“What convinces the company is of course a different price than that of our on-premise solution.”
Buyer06	“So how we exchange data with our customers. This could be done very well with a cloud.”
Buyer07	“Certainly, in all discussions, wherever the word cloud is used, all players, stakeholders, everyone involved, has difficulties with it.”
Buyer08	“In terms of reliability I trust them equally. Because that’s their business model.”
Buyer08	“Because I get a solution in the cloud and not only cloud space, this is what makes sense to me.”
Buyer08	“I believe in this business model, then I have an advantage.”
Buyer09	“This does not mean that we are always last with new technology, no, but we actually want to build on things that are already mature. We don’t have to be the pioneers and get bloody noses”.
Buyer11	“I mean I trust the cloud, but I want to go through the certification process. To confirm that I mitigated my risk.”
Seller04	“I think that the cloud industry has immense potential in Germany which is currently unexploited.”
Seller06	“Nobody is doubting our technological capabilities anymore, that one of the large cloud providers would not get a grip on it from a technological point of view.”

Seller07	“There is no doubt that the future will be in the cloud.”
Seller07	“Question is if it has a positive impact on the business. This is in Germany still a huge discussion point.”
Seller08	“This changed a lot over the last years. My customers see cloud computing as a big future of their IT. Mostly through agility advantages. This might not be true for all companies.”

U.S. cloud services, features and maturity

Interviewee	Quote
Buyer01	“The American provider may be 2, 3, 4 years ahead of the German cloud solutions.”
Buyer02	“The main difference is usually the price.”
Buyer03	“As I mentioned before, it is clear that the major IT players are based in the US. Companies such as Microsoft and Amazon alone, according to press reports, are investing multiple times the sum of money in data centres than the total revenue of their German competitors. In this respect, you can already see the power behind it. […] But there are no solutions form German companies that can compare to solutions from companies such as Microsoft. These are small providers, niche suppliers, partially medium sized companies, with quite clever solutions, but nothing a company with 40 billion euro in revenue could rely on.”
Buyer05	“I can’t think of any alternative which is as comprehensive, with what is being offered, with Lync, with OneDrive or how it is called, I’m not sure if there is another provider with a similar offering.”
Buyer06	“Well, let me put it this way, the major IT trends do not come from Europe, they come from America.”
Buyer08	“I believe this doesn’t exist in Germany. For this reason, the cloud topic only makes sense for me with Microsoft.”
Buyer11	“What some of the Chinese providers are doing… I wouldn’t be surprised if Alibaba starts selling cloud web services anything different than Amazon. That would not surprise me.”
Buyer11	“And there are not that many Germany based software development companies. I mean there is Software G, there is SAP… And in order for SAP to compete they need to come up with a cloud for that part of the world, while at the same time they can demonstrate that they have data protection for this part of the world.”
Seller01	“European providers are hoster, re-labelled in cloud hoster or cloud provider.”
Seller04	“The solutions of the American manufacturers are generally regarded as the market leaders.”
Seller05	“The products of U.S. companies, especially CRM, are considered to be better than German or European products. The Americans have proven the maturity of the products with millions of users.”
Seller06	“I can’t come up with a notable German cloud provider. Maybe SAP, but they also made many acquisitions.”
Seller07	“The huge difference between U.S. versus German vendors is that most new technologies come from the US.”
Seller07	“All offerings which are offered in Germany and don’t come directly from the vendor will only be a subset of what you get from the original vendor.”
Seller08	“They see that the U.S. companies are the market leaders and if you want to do serious cloud computing today you have to use the U.S. cloud services. Only these companies give you the speed of development and speed of innovation.”
Seller08	“They think they have no choice but to use U.S. vendors. There are not really any serious competitors in Europe or Germany. Only in the start-up-space for cheap virtual machines but not in the enterprise market.”

Shadow IT

Interviewee	Quote
Buyer02	“I believe that our IT policies are sometimes handled a little lax so that things such as Dropbox are used occasionally.”
Buyer07	“Well, in the past we set the technology standards, we provided them, from the corporate point of view. Now it is more coming from the consumer, from what I use at home.”
Buyer08	“Because I believe that I anyway cannot prevent this part that you just mentioned.”
Buyer08	“These banal examples show me and prove to me that it is more important to change the process and the handling of the data rather than making technology available to regulate this somehow.”
Buyer09	“Our employees are doing things that we cannot and don’t want to prevent.”
Buyer09	“We have our own cloud which you can use and which we of course favour for company data. This is actually obligatory. But I’m sure that there is still somebody who is just doing it differently.”
Seller05	“This is also a good approach to sell that: You are surely using cloud, you just didn’t know about it yet.”
Seller07	“Sometimes the customers don’t really want to talk about it with us as a vendor. This is something which is from their point of view only an internal matter and needs to be discussed internally. However, they know that they don’t have any internal alternatives, but they see the risk of data leakage.”
Seller07	“Often the senior management is themselves working with non-compliant devices and services.”

U.S. cloud providers

Interviewee	Quote
Buyer01	“The American cloud providers can do little if the American government is not doing anything. They are subject to the underlying legislations which they cannot shake off.”
Buyer03	“I cannot even trust the statements of the chief executives of those companies since they are partly obliged by law to lie. This is because of the national security letters.”
Buyer03	“Ultimately, it is not just about where the data is hosted, because American technology is built in everywhere, HP, IBM, Apple, Dell and the rest of them, if I’m not bugged on the upper layers of the ISO/OSI model, they can get me somewhere on the lower levels. This means that it is extremely difficult to escape from this data kraken.”
Buyer03	“So, if you take this whole package altogether, I just have to say that, at the present day, I wouldn’t be able to trust an American company with my data with a clear conscience.”
Buyer03	“I believe that the U.S. companies would prefer to get this issue off the table and to carry on with their work as they used to, but they are, however, in a juridical dilemma.”
Buyer03	“In principle, the logic would indeed make a lot of sense, however, how does that help me when the technical configuration as well as the formal contracts are secure, but there are huge holes in the background where information can leak out?”
Buyer04	“I’m not in the position to tell if the outcry of these companies in the press is just practiced marketing.”
Buyer04	“If I had the choice I would always go to a German or European company where I know that the Americans have no access to it.”
Buyer04	“If I could do what I wanted to do I would throw out a lot. If it made economic sense, I would replace all sorts of U.S. products.”
Buyer04	“They do not have any chance to defend themselves; the weakest link in the chain is trust, right?

Buyer04	“I would know that U.S. intelligence services had full access to my data. Therefore, I would reject this wherever possible.”
Buyer05	“I think that the NSA would be able to decipher and read our emails no matter where they are stored.”
Buyer05	“The cables belong to someone and if they are sitting at the end of the cable, they can make the emails available to somebody. It doesn’t matter if it is Microsoft or if it is Cisco capturing something through a router, whatever, we cannot prevent that.”
Buyer05	“Therefore, I would assume that Microsoft is on it, that Oracle is on it, and all the others. I would be more surprised if they would not be on it.”
Buyer07	“I believe that they cannot do anything substantial.”
Buyer07	“When one hears that there has actually been some cooperation between companies such as Apple and Google with relevant institutions, state bodies… this is in my view a new quality where they ultimately set their own business model at stake.”
Buyer08	“I trust Microsoft 100% that they do not have any intrinsic motivation to hand over the data. Why? If they wanted to do that, they could have done it a long time ago”.
Buyer11	“Exactly, you may trust the cloud provider more than you trust the government.”
Buyer11	“Because I can sue the cloud provider if there is any data leakage. I can equally sue the government. But I may be more successful If I sue the cloud provider. Because they have a profit motive and the government is just there for other purpose.”
Seller05	“I don’t believe that U.S. companies are interested in doing that.”
Seller06	“The large majority of Germans only sees the NSA topic and wants to keep their data in Germany.”
Seller06	“I’m always telling them that there are no backdoors and that we were as angry about the NSA surveillance activities as everybody else was.”
Seller07	“It’s the question of law. Everybody is aware that we need to fulfil the law in each country. We have these discussions.”
Seller07	“It’s not so much the U.S. companies but more the US government. They trust US cloud providers but they don’t trust the US government.”
Seller07	“If we encrypt with customer keys or unique keys it would work. Otherwise, as long as we have the opportunity to decrypt it, for sure we have to do it if we are asked to. As long as there is a master key there is always the chance that we have to use it.”
Seller08	“The trust also depends on the U.S. company. For example, Google has less trust than the other big two.”
Seller08	“Most customers understand that crimes like terror must be fought and that is OK to get access to the data when serious crimes need to be investigated. But here is still distrust that the US government would use the data for other purposes.”

German cloud providers

Interviewee	Quote
Buyer02	“I would say that this is very much driven by fear. I believe that, especially with our large customers, it is generally not based on a legal background.”
Buyer02	“But there is just an insane phobia to not even come anywhere near of this danger that such a thing happens and therefore they are very strict in this matter. On the other hand, it certainly has something to do with the fact that they can use that in turn as a marketing argument.”
Buyer02	“Firstly, it is a requirement from the customer to us. And secondly, by transforming this requirement into a feature, we can differentiate ourselves from the competition.”
Buyer04	“I believe the trust in German products is much higher than in the average of European products, if this is even reasonably possible.”
Buyer05	“Even if a German product would be developed from scratch and made available to the people, I don’t know if it could provide absolute security.”
Seller04	“German and European companies are more appreciated regarding data privacy. SAP etc. will certainly be more appreciated.”

Seller05	“It led to the fact that German providers, for example the Telekom, are pushing cloud in Germany. There are many small providers, which would not exist without the NSA issue, that are trying to fill that gap and that are successful with some customers.”
Seller06	“Cloud Made in Germany became a sales argument. Nobody cares if this provider has already been hacked before.”
Seller06	“The German hosting companies certainly benefit from the situation.”
Seller07	“You can see it everywhere. This is the only advantage they have. They have no chance to convince with functionality. They have only the chance to beat us regarding the access of data.”
Seller08	“There were German cloud providers and outsourcers and hosters, that call themselves cloud providers, in my experience with not so much success. While they have advantages on the legal aspects, they are missing most of the features that you can get from the big U.S. providers.”

Private cloud

Interviewee	Quote
Buyer04	“I might be inflexible in the traditional European countries, but if I increase the number of staff in Mexico, Malaysia, India and China, I’m just as flexible as with an external contract with relatively short periods of notice.”
Buyer05	“Because we’re saying that there are departments which are that strategic or important that we don’t even accept the slightest risk that someone look in there.”
Buyer06	“There is no reasonable security solution for the cloud. Once I’m in the cloud, I’m in an uncontrolled space, in a legal vacuum.”
Buyer08	“I do not need a hosting service; room size does not matter anymore. When a large enterprise looks at how much space they need today for the same computing power they needed 10 years ago, you know this example from the IBM ads. This cannot be a cost factor anymore.”
Buyer08	“I don’t really know if the cloud topic is clearly defined in the heads of the people who are talking about cloud”
Buyer09	“Where it is of course getting exciting is whenever we have personal data, for example our payroll. We won’t put that in the cloud, that we keep in-house.
Buyer10	“I’m very cautious about it, mainly just because I prefer to have all our labours under our direct control, rather than outsourcing. It is more an outsourcing versus an insourcing question than a cloud versus non-cloud question to me. So, I start from the business aspect that I prefer to have all the labour under our direct control.”
Buyer10	“So, he understands my business very well and now he is running the run-side of the business, so I’m very trustful of that relationship.”
Buyer10	“I think the other thing, and amongst all of it, I guess it is partly under the trust point you make, is who do you call when something goes wrong?”
Buyer10	“So, my whole point… a little bit long winded, sorry, my whole point is that I don’t necessarily distrust the cloud, it is just that I trust what I have to a great degree and therefore it has to overcome that. It is more a positive statement about trust as supposed to a distrust statement.”
Buyer10	“People talk a lot about it saving cost, but I haven’t really seen it. Because we have pretty good scale in our data centres anyway, how much cost can we really save?”
Buyer11	“When we look at those two different workloads, commodity cloud is something that you can be doing via any cloud provider. You know for example Microsoft Yammer as a blogging tool, as a commodity cloud, consumption-based solution.”
Buyer11	“The other spectrum of it is the mission critical loads. And those mission critical loads, for example the contracts logistics information system is core of one of our business divisions. That we will never put on a public cloud. We will move that to a cloud but that will be an on-premise cloud.”
Buyer11	“The other thing that we have learned from experience is that even with a public cloud provider you still have information security breaches. And we had that experience already.”

Buyer11	“You can defend yourself equally well. The thing that you don’t know is what business users are working at that system. When you’re hit, what’s the impact?”
Seller06	“The trust in the local data centre provider is still high in Germany.”
Seller07	“If you talk about access with the customer, they understand that they cannot compete with cloud security.”
Seller08	“When it comes to data security and privacy of data, companies tend to have a significantly higher trust in their own IT organisation than in any external vendor. This is in my view not valid since most data leaks come from inside and not from outside.”
Seller08	“On the other side, in general, customers have less trust in their own IT organisation when it comes to agility and scalability than in an external cloud.”

Local sales representatives

Interviewee	Quote
Buyer03	“They are desperate to find arguments to defuse the threat situation, but I haven’t heard a single argument that would convince me.”
Buyer03	“American companies are traditionally highly centralised and controlled from the USA. I have witnessed that myself at HP.”
Buyer03	“I recently negotiated a contract with IBM where I experienced that they had to ask over the great ocean for approval for every fart.”
Buyer04	“Not at all. Even if they were the most reputable and most honest citizens I could think of, none of them can guarantee anything.”
Buyer05	“Some are nice, they are all sales people, but I don’t think that this had anything to do why we chose them.”
Buyer05	“I would imagine that if he would have been completely unsympathetic, we might have kicked him out eventually, but it wasn’t the case that we wanted to do him a favour or this didn’t have anything to do with it.”
Buyer09	“And what the technology can really do is often not what the sales person promises. In my opinion both have to be on board. The technicians must speak with the technicians here.”
Buyer10	“I think it is more about the responsiveness of the organisation and understanding my business. Because like all of us you can’t rely on one person in today’s world, right, especially in our organisation, when we are a global 24/7.”
Buyer11	“My experience is, and this is my own experience, I have spent three years now in Germany, that when it comes to those kinds of things, I want to talk to somebody in the home organisation.”
Seller01	“You can speak German with the customer in Germany, which is an advantage.”
Seller02	“Nothing happens here without the first handshake.”
Seller03	“A personal conversation is very important to understand the biggest pain in the company.”
Seller03	“It’s a business between people, the technology then fades into the background”
Seller04	“Only small businesses buy directly online. Larger companies prefer a personal contact who they can talk to.”
Seller05	“It helps enormously if you speak German.”
Seller06	“This is definitely a competitive advantage when there is somebody in the field, when the people have a face. Most people only know us online.”
Seller06	“I have not hired anybody yet who did not speak German.”
Seller07	“Customer have a lot of questions. They would not ask these questions if it was not about cloud from a U.S. vendor.”
Seller08	“This depends on the customer. Traditional German customers would require a local contact person whenever they need somebody to talk to get technical or sales advice. The enterprise customers would not buy U.S. cloud services without a local sales representative.”
Seller08	“My start-up and media customers like to do everything online and they don’t need local representatives as long as their online-presence and support are good.”

Market and sector knowledge

Interviewee	Quote
Buyer07	“Somehow, I also believe that a company has a certain philosophy and follows it through, let’s say, recruitment, personnel selection, personnel qualification, which should also be considered.”
Buyer08	“But I would not trust an Amazon employee that he understands my business and takes care of me. Admittedly I’m relatively old-fashioned and I believe that humanity is in general old-fashioned on this point.”
Buyer08	“No matter what… for example coffee cups, tables, no matter what you pick, clothes, doesn’t matter. I need this trust, and this is of course always personified in a contact person.”
Buyer10	“It’s more about… does the organisation get what we kind of trying to do, and yes, of course, you need to have some context. So, when shit hits fan you can pick the phone up. That is more about, you know, is that third party got the right philosophy, do they have the right spirit, have they got the right, you know, that fits what we’re trying to do.”
Seller07	“It is important to have references in the sector or industry to convince the customer.”
Seller08	“The biggest trust customers have is in other peers in other companies. As soon as they see that their peers have trust they are ready to trust cloud providers. Success stories help significantly, get customers together and talk about their experiences, etc.”

Global surveillance disclosures

Interviewee	Quote
Buyer03	“I believe that sometimes you have to openly call a spade a spade and make clear that what happened since 2001 caused a gigantic damage.”
Buyer03	“Laws were bent and broken in the background and who can promise me that this will change in the future? According to the motto: A liar will not be believed even when he speaks the truth.”
Buyer03	“Basically, all American companies are affected by this topic and I honestly don’t know how they could win back the trust they have lost.”
Buyer03	“But as I said, for me, this process will take years, if not decades. Lost trust, especially in this area, cannot be regained that quickly.”
Buyer03	“The worst part is that there is no open communication about what is happening and therefore you cannot trust anyone anymore. At this point you can only try to protect your data as effectively as possible and choose a provider which is probably not yet infested, or which is not of interest for the NSA.”
Buyer04	“I believed that I had a relatively realistic view on this matter, however it has been corrected to such an extent”.
Buyer04	“Also, the technical possibilities, back doors in Microsoft products, this has been discussed forever. All of this is reality, all became proven reality.”
Buyer06	“So, when we add all of this up it was really a huge thing… what came out was a real blow.”
Buyer06	“This was the most expensive mobile phone in Germany, yes, entire departments have been dealing with it. This was no mobile phone from the shelf which has just been modified but it was specifically built for Mrs. Merkel… bugged!”
Buyer06	“Currently, the USA is a very difficult topic. I cannot imagine that this would be possible right now considering NSA and Co. Which means: no.”
Buyer06	“First of all, it caused unrest and agitation, and everyone has to find out where they are standing regarding this issue. How secure am I?”
Buyer07	“I would say that the overall sensibility increased.”
Buyer08	“I believe that the U.S. and the authorities such as the NSA are in this point much more advanced than the BND.”

Buyer11	“What is going to be done with that data? How will that data going to be used to my advantage or to my disadvantage?”
Buyer11	“And that is why we also make it a point to take all of our data and all of our servers out of those countries. To not give them, you know, we have chosen two neutral countries, one in Europe and one in Asia.”
Seller03	“The Snowden topic did have an impact on the business.”
Seller03	“The NSA topic is very emotional.”
Seller03	“The Snowden topic comes from the hardboiled.”
Seller04	“From my experience in the German speaking countries, the NSA revelations destroyed the trust.”
Seller04	“The business slowed down in Germany. It was very weak already and slowed down even more.”
Seller04	“The U.S providers are not able to protect the data from things like the PATRIOT Act which caused that a lot of trust has been lost in the solution.”
Seller05	“I don’t know anyone who didn’t address it. I believe that it depressed the cloud business.”
Seller06	“Everyone was mad that the wires had been tapped. It definitely caused great frustration, it was of course a crazy topic.”
Seller06	“This also had a negative impact on our business.”
Seller06	“It is, however, difficult to say because the cloud topic was already difficult in Germany before. Snowden reinforced this general distrust, but it already existed earlier.”
Seller08	“There were always people who said that you cannot trust the U.S. government. Snowden proved that they were right and that everybody in the entire world was spied upon. This was a big issue for all cloud providers.”
Seller08	“The second thing that Snowden did was to make transparent the scale of the spying. Nobody expected that all the communication is recorded and monitored and that the agencies had the capacity to do that. It’s the scale of the spying that had a great drawback on the cloud industry.”

Economic espionage

Interviewee	Quote
Buyer01	“Personally, I consider economic espionage as the greatest danger”
Buyer02	“As an [advertising] agency, our fears about the tapping of trade secrets are relatively low. […] I believe that there is a much higher security awareness in other sectors. BMW is for example a completely different world.”
Buyer03	“One can hence assume that not even everything is known which is happening in the background and I think that American intelligence services, when you look at the history of the CIA, which is active abroad, use the collected information also for the benefit of the U.S. economy. Or that certain CIA activities were only undertaken because they served the U.S. economy.”
Buyer03	“We have found Trojans and other things where white-collar criminals tried and probably are still trying to spy on us. And because intelligence agencies are doing this with completely different financial and technical capabilities, they are able to crack 128-bit encryption with some computers in the background, etc.”
Buyer03	“I will certainly not save any business-critical information, such as data on development projects, data on the corporate strategy, data about key people like business managers, in the cloud but would always try to keep them locally.”
Buyer03	“There is no absolute protection, you can only try to make it as difficult as possible for those guys.”
Buyer03	“I believe that it is somehow not opportune in Germany to stoutly take advantage of the economic policy or intelligence agencies to benefit the domestic economy. Maybe because we are a bit ashamed. I believe that with the Americans, the Anglo-Americans, including the French cultures, it just is like this.”

Buyer04	“A few years ago, I would have said no, but there were some examples where it actually came to the surface, where data demonstrably disappeared and was used by U.S. companies to their advantage.”
Buyer04	“I believe that other companies are much more sensitive, quite rightly much more sensitive than us.”
Buyer06	“I don’t know; I wouldn’t rule anything out. Ultimately, it’s about economic interests, it’s always about economic interests. Hence politics also serves the economy.”
Buyer07	„But again, personally, I would consider it neither impossible nor unlikely that government agencies are supporting the economic interests of American companies.”
Buyer08	“What process are we talking about and is this information that we are sharing confidential? And is there enough motivation from a third party to tap this information because it gives them an advantage?”
Buyer09	“Now when we talk about company data… when ZF develops something, or Siemens, this is probably worth a thousand times more than… what we work with?”
Buyer10	“I don’t know if other industries are concerned about that, and that’s why for example, in manufacturing, one of the reasons why you see a trend back to manufacturing at home for some industries because they are concerned about IPR.”
Buyer11	“Yes, there is that fear. We don’t know.”
Seller03	“The topic economic espionage is important.”
Seller04	“Many customers in the R&D area would never put this data in the cloud.”
Seller05	“Especially machine engineering, well, almost solely machine engineering, are addressing this issue and are clearly saying that the Americans are practicing economic espionage. They fear that they lose their know-how. Unfortunately, I don’t have a satisfactory answer for that.”
Seller06	“We already had this topic on large customer events.”
Seller06	“This is partly a confusion and I think that it is dangerous to educate the German SME and make them believe that his data was necessarily secure because it was stored in Germany.”
Seller07	“Highly confidential data is encrypted with their own keys or they have it on-premise under their own control.”
Seller08	“In engineering companies yes, not so much in media or other industries. I heard that several times from engineering companies.”
Seller08	“There is also a new development after the Volkswagen Diesel-gate case. Companies fear that their data can be used against them in lawsuits.”

U.S. government reactions

Interviewee	Quote
Buyer03	“One does not even know if they are still in control or if they are just overdriven by people in the background, from the intelligence agencies. This is one more of these elements of uncertainty.”
Buyer04	“I wouldn’t trust them anymore, because this is a question of attitude. I would sit back, wait 5-10 years and see how much I can still read in the press about this.”
Buyer05	“But the most critical point for me is definitely the abolition of the statutory duty of the collaboration between the authorities and the U.S. companies.”
Buyer06	“They could no longer hide it, and they have not really actively prohibited it and not acted proactively, no. The power interests are stronger. And the American arrogance.”
Seller03	“There is the wish, that the U.S. government becomes less deeply involved.”
Seller05	“It would be best if the U.S. government would shut up.”
Seller06	“I believe that the trust has certainly been forfeited.”
Seller07	“I have a doubt that there will be a change. The organisation and communication might change but the impact will be the same.”

German and EU government reactions

Interviewee	Quote
Buyer01	“There is, however, much going on in the background, and I must also say that, since we just had this discussion in our regular department manager meeting, I can clearly see the trend away from the freedom of globalisation back to the old nation-state mentality.”
Buyer03	“However, when I can choose, we are currently trying to stay in Germany [with our data] because of the German data protection legislation, yes because we have more trust in it than in the EU legislations… […] In this respect I can be sure that German law applies. I will never be able to tell if there is not also somebody in the background who is trying to bypass the law, but at least the overall conditions are in place that I can rely on.”
Buyer03	“One must exert pressure; it will not work without pressure. And this pressure can only come from economic indicators, incoming orders, sales revenue of U.S. companies, etc. Pressure can only be generated this way.”
Buyer03	“I think that if these economic disadvantages occur, this is the only way to start a change process in the American government.”
Buyer03	“If you look at it, Siemens had computers, they had mobile phones, they hat computer chips, they had semiconductors, they had IT, Siemens successively sold all of it.”
Buyer04	“One part of this finding is that our intelligence agencies can also do what they like. They are accomplices. I can’t see any real attempt of our federal government to clarify this matter.”
Buyer05	“If they are not able to put pressure on them then I don’t see any possibilities how they could help.”
Buyer07	“Well, therefore I think… one could also say… that’s not even long ago what Mrs Merkel said about the Internet, that we are slowly… that we are still at the beginning… that actually shows that we are to some extent running to catch up with the process.”
Buyer08	“And again, I believe that Germany cannot handle the issues of data protection, data rights and the Internet. We don’t have… at least what you hear when politicians speak… I’m missing the skill behind that.”
Buyer09	“The German government? Please stay out of this! I’m serious, because they do not understand this. The government will probably go in the wrong direction and there are enough competent people working for companies in Germany and Europe that can drive this topic. I’m sceptical whenever politicians intervene.”
Buyer11	Yes, I mean… I think… and the reality is that the German government and the U.S. government they are not trusting each other. Never mind wiki leaks or Snowden… the fact is that there has been wire-tapping or listening on a conversation of senior German officials. And they have been caught. So, there is a lack of trust on the Government level and that lack of trust also moves to lower levels.”
Seller05	“It’s about time that the Europeans come to an agreement with the Americans.”
Seller06	“Germany should support more start-up companies and provide more investment capital. The politicians should ask themselves how they can effectively secure Germany’s position as a high-tech location.”
Seller07	“We are working actively with the regulators of the EU. We are very transparent with this. The problem is the confusing and complicated federal IT compliance system in Germany.”

Data centre location

Interviewee	Quote
Buyer03	“According to the PATRIOT Act, there is also unrestricted access to data in offshore data centres of U.S. companies, even if it contradicts with local legislation. It is a step in the right direction, but it does not really solve the problem.”

Buyer03	“Although, if I could choose, we would try to stay in Germany (with our data), because of the German data privacy act … yes because we have more trust in it than in the EU legislation… In this respect, in Germany I can be sure that German law applies.”
Buyer04	“Even if Microsoft has a data centre in Ireland, they can still not guarantee that U.S. intelligence services have no access to the data.”
Buyer05	“In Germany, you just always have the feeling that it would be safer because it is located in Germany, but this is only a feeling and I don’t think that this is somehow founded.”
Buyer06	“I’m assuming that if IBM is building a data centre in Germany, the owner is a German subsidiary of IBM which is then subject to German law. And German law is also legally enforceable.”
Buyer06	“The subject ‘data’ is sacred at Company06. Data of Company06 are in general stored in Germany. There is actually no discussion about using service providers that store data outside of Germany. Data of Company06 stays in Germany.”
Buyer06	“Definitely the topic data protection and data security. In Germany, we have to my knowledge the most far-reaching data privacy act. And there are hardly any countries on a similar level in Europe.”
Buyer06	“If all parameters are the same, we would decide for the German option.”
Seller03	“One of the first questions is: Where is the data stored?”
Seller04	“A data centre in Germany is definitely confidence-building measure.”
Seller05	“The data centres in Germany are very important so that the data is stored in Germany.”
Seller06	“I would probably offer the storage of data in Germany as an option, but, eventually, it needs to be more expensive. An overhead should then also cost more.”
Seller07	“Most customers would like to use a German data centre and have their data in Germany. But it might reduce the functionality and scalability of the solution.”
Seller08	“And if it is handled by German citizens the trust is higher than if it handled by U.S. people.”

Legal proceedings

Interviewee	Quote
Buyer03	“In order for me to believe them they would really have to go to the barricades to fight back against these compulsory measures.”
Buyer04	“I believe that this is in any case the right approach. However, as I tried to say before, I wouldn’t be able to distinguish or tell if this was part of a marketing campaign or if this was really serious about that.”
Buyer06	“I would say that this is definitely helpful. Yes, but this is certainly not conclusive, it could also be a press or marketing gag, but it is helpful in any case, for sure.”
Seller04	“It is very important to show that the concerns of the Germany and Europeans are observed and to show that one is responding to it.”
Seller05	“It is also important to oppose the US government practices and to claim one’s due.”
Seller08	“I would have expected customers to ask for that. But I do not see so much interest by customers. In my experience customers don’t really care.”

Cloud computing contracts

Interviewee	Quote
Buyer02	“Plus, a contract that most company lawyers do not really understand, but where you have to consult a specialist.”
Buyer03	“As I can see today, contracts are being bent and broken. All these stories, formal assurances, without any changes in the background to the PATRIOT Act and all these things, are merely window dressing.”

Buyer08	“And, to answer your question, the company that really listens and not only says that they are listening will have an advantage.”
Buyer09	“I do not read 50 pages of terms and conditions. I do not understand that. If I need a lawyer to do that… Preferably a contract fits on a beer mat. It needs to be understandable.”
Seller01	“Contracts need to be made up according to German law.”
Seller02	“American companies don’t like to do that.”
Seller07	“The wishes are high. But the main reason is that German customers only know German law. Another key main reason is warranty and liability. Based on German law you need to have an unlimited liability. We cannot do that with a cloud service.”
Seller08	“My feeling is that customers want to have everything local. The less they have to deal with the bigger their interests are in cloud.”

Data encryption

Interviewee	Quote
Buyer01	“The NSA is not stupid and can prevent many technical possibilities. That’s a hare hedgehog game. Even if you build in a lot of security, eventually a clever person with the necessary funds and the necessary working environment will find a hole.”
Buyer05	“That was an important criterion. If we were not able to encrypt the way we did, it would certainly not have happened that way. Then we would not have done it.”
Buyer05	“Many things that we are sending back and forth by email could be read by somebody without hurting anyone, without hurting the company. And anything that could hurt the company needs to be encrypted anyway...”
Buyer07	“When you smuggle drugs, yes, then there is a haptic good, yes, and one can eventually find it or not find it, or something. However, I would say with data you do not know… according to the motto… you can actually only hope that somebody will find it somewhere, etc.”
Seller01	“This is not a free ticket for the cloud consumer but a model of dual responsibility.”
Seller06	“Encryption is always a topic, but it also creates new challenges for both parties.”
Seller08	“Encryption is a very hard topic and U.S. cloud providers should make it much easier for their customers to use it in order to gain trust.”