The University of Strathclyde
Humanities and Social Sciences Department
Law School

How is User Trust in Cloud Computing Affected by Legal Problems Relating to Data Protection in Cloud Computing? And How Can User Trust in Cloud Computing be Built?

Auntika Na Pibul

Submitted in fulfilment for
the degree of Doctor of Philosophy
2019

DECLARATION

This thesis is the result of the author's original research. It has been composed by the author and has not been previously submitted for examination which has led to the award of a degree.

Sign: Auntika Na Pibul

Date: 17/12/2018

ABSTRACT

Over the past few years, cloud computing has become an increasingly popular service, providing Information Technology (IT) resources over the Internet. Many types of cloud services, ranging from simply offering an outsourced storage to a full external provision of hardware infrastructure is the main factor attracting people to adopt cloud computing. Nevertheless, the distinctive features of cloud computing pose some privacy and data protection (DP) risks to cloud users, and these risks have become their major concerns.

Especially after the revelations about the United States (US) government's mass surveillance programme in 2013, many surveys have shown that individuals and small and medium-sized enterprises (SMEs) have been hesitate to entrust their data to cloud service providers (CSPs), especially to CSPs controlled from the US or which have servers located within the US, because their trust is affected by those risks. Accordingly, a range of CSPs, e.g. Google and Microsoft, have tried to build user trust in cloud computing by offering a variety of DP and privacy assurances.

This situation may yet prove to be a tipping point in terms of showing how willing users are to place trust in cloud computing. As cloud computing has great potential to improve productivity and innovation, this lack of trust could affect the economic development not only of EU societies but also global societies as a whole, so that building user trust in cloud computing needs to be accomplished in order to increase the use of cloud computing.

As legal problems relating to DP in cloud computing do pose risks and uncertainties for the privacy of EU cloud users, this thesis aims to explore how user trust in cloud computing is affected by these problems. However, this thesis focuses on just two main legal problems relating to DP: (1) legal problems regarding the application of the EU DP law to the processing of personal data in the cloud; and (2) legal problems regarding the EU and US legal frameworks governing access to personal data held in the cloud by law enforcement and national intelligence agencies.

With regard to the theory of trust and a number of surveys showing the reasons why individuals and SMEs feel reluctant to place their trust in cloud computing,

whether or not individuals and SMEs trust cloud computing seems to depend on three main factors: (1) transparency and control; (2) accountability; and (3) security. This research shows that the two legal problems identified do have an adverse impact on these three factors, as they (1) raise a number of uncertain issues, which then make it difficult for cloud users to exercise control over their data; (2) make it unclear whether CSPs will be held responsible and accountable for the personal data processing; and (3) pose security threats to personal data residing in the cloud. Finally, this thesis concludes that the two legal problems affect user trust in cloud computing, at least to some extent, and that this situation could potentially impede the use of cloud computing.

As a result, this thesis proposes both legal and non-legal approaches for building user trust in cloud computing. The legal solutions are mainly drawn from the new EU DP law (General Data Protection Regulation(GDPR)). Due to the fact that trust is a very subjective matter and it takes time for it to be built, legal approaches alone may not be powerful enough to build and/or rebuild trust in cloud computing. This thesis also proposes non-legal solutions (1) for enhancing transparency and ability to control over the data, i.e. icons and labels and transparency reports; (2) for improving accountability of CSPs, i.e. certification, trust marks and trust seals, internal codes of conduct or ethics; (3) for increasing security of data, i.e. technical approaches and localised cloud computing, as they are likely to help boost the possibility of individuals and SMEs placing their trust in cloud computing. All these approaches aim to fulfil three criteria for creating trust in cloud computing, as listed above, in order to enable users to be less concerned about their data residing in the cloud and let them be sufficiently confident to ignore any risks that might stem from those two legal problems and thus to be willing to place their trust in cloud computing for the sake of benefiting from its advantages.

ACKNOWLEDGEMENTS

I would have never been able to complete my thesis without support from a lot of people which I would like to acknowledge and give particular mention. My deepest gratitude and appreciation goes to Professor Lilian Edwards for being such a supportive supervisor. The extensive knowledge of Professor Lilian in the fields of data protection law, and internet law has been the source of my inspiration throughout this thesis. I would like to express my sincere gratitude to her for her guidance and continuous and unrelenting support. I was continually amazed by her excellent comments which were extremely useful for my thesis. A very special thank you to Prof. Kenneth Norrie and Dr. Lorna Gillies for useful comments on this thesis. The completion of this thesis would not have been possible without the scholarship I received from the Royal Thai Government. I would also like to thank the National Institute of Development Administration (NIDA) for providing the funding which allowed me to attend interesting conference.

Lastly, I am grateful to my dear family for their unconditional love, support, understanding and encouragement. I would like to dedicate this piece of work to my father, mother, my grandfather and my grandmother.

TABLE OF CONTENTS

LIST OF FIGURES & TABLE

CHAPTER 1

INTRODUCTION TO CLOUD COMPUTING

CHAPTER 3

LEGAL PROBLEMS REGARDING THE APPLICATION OF THE EU DATA PROTECTION LAW IN CLOUD COMPUTING

CHAPTER 5

SOLUTIONS TO THE LACK OF USER TRUST IN CLOUD COMPUTING

LIST OF CASES

CJEU case

Case 168/84, *Gunter Berkholz v Finanzamt Hamburg-Mitte-Altstadt*, ECR 2251, ECJ, Judgment of 4 July 1985.

Case C-390/96, *Lease Plan Luxembourg v Belgische Staat*, ECR I- 2553, ECJ, Judgment of 7 May 1998.

Case C-101/01 *Bodil Lindqvist* v *Åklagarkammaren i Jönköping*, ECR I-12971, CJEU Judgment of 6 November 2003.

Joined Cases C-585/08 *Peter Pammer v Reederei Karl Schlüter GmbH & Co KG* and C-144/09 *C Hotel Alpenhof GesmbH v Oliver Heller*, CJEU, Judgment of 7 December 2010.

Case C‑543/09 *Deutsche Telekom AG v Bundesrepublik Deutschland*, CJEU, Judgment of 5 May 2011.

Case C-190/11 *Daniela Mühlleitner v Ahmad Yusufi and Wadat Yusufi*, OJ C 204, CJEU, Judgment of 9 July 2011.

Case C–131/12 *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD*), Mario Costeja González, CJEU, Judgment of 13 May 2014.

Case C-230/14 *Weltimmo S.R.O. v Nemzeti Adatvédelmi és Információszabadság Hatóság,* CJEU, Judgment of 1 October 2015.

Case C-362/14 *Maximillian Schrems v Data Protection Commissioner*, CJEU, Judgment of 6 October 2015.

Case C‑191/15 Verein für Konsumenteninformation (VKI) v Amazon EU Sàrl, CJEU Judgment of 28 July 2016.

ECHR case

Handyside v.UK, no. 5493/72, ECHR, 7 December 1976.

Dudgeon v. UK, no. 7525/76, ECHR, 22 October 1981.

Malone v. UK, no. 8691/79, ECHR, 2 August 1984.

Olsson v. Sweden (no.1), no.19465/83, ECHR, 24 March 1988.

Moustaquim v. Belgium, no. 12313/86, ECHR, 18 February 1991.

Andersson v. Sweden, no. 12963/87, ECHR, 25 February 1992.

Niemietz v. Germany, no.13710/88, ECHR, 16 December 1992.

Keegan v. Ireland, no. 16969/90, ECHR, 26 May 1994.

Kroon and Others v. the Netherlands, no. 00018535/9, ECHR, 27 October 1994.

Bensaid v. UK, no. 44599/98, ECHR, 9 February 2001.

Leyla Sahin v. Turkey [GC], no. 44774/98, ECHR, 10 November 2005.

Dumitru Popescu v. Romania(no.2), no. 71525/01, ECHR, 26 April 2007.

Bykov v. Russia [GC], no 4378/02, ECHR, 10 March 2009.

Hartung v. Germany, no. 10231/07, ECHR, 3 November 2009.

Others

Edwards Hasbrouck v US Customer and Border Protection, US District Court for the Northern District of California, San Francisco, C 10-03793 RS, Judgment of 23 January 2013.

Facebook Inc. and Facebook Ireland Ltd. v. ULD, 8 B 60/12 and 8 B 61/12, German Administration Court, Judgment of 14 February 2013.

Mary-Rose Harkin v Edward Towpik & Ors, High Court Northern Ireland (IE), IEHC 351, Judgment of 22 July 2013.

Facebook Ireland v Hamburg Court of Appeal, VG Hamburg, 15 E 4482/15, Judgment of 3 March 2016.

Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, No 4809 P, High Court of Ireland, Judgment of 19 July 2016.

Case T-738/16 *La Quadrature du Net and Others v European Commission*, the EU General Court (Second Chamber), Judgment of 9 January 2017.

Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, No, 4809 P, the Irish High Court, Judgment of 3 October 2017.

Case T-670/16 *Digital Rights Ireland v European Commission*, the EU General Court (Second Chamber), Judgment of 22 November 2017.

LIST OF ABBREVIATIONS (TECHNICAL TERMS)

CSPs	Cloud Service Providers
DAC	Discretionary Access Control
DRMs	Digital Right Managements
EC2	Amazon Elastic Cloud
ECS	Electronic Communication Service
GAE	Google App Engine
IaaS	Infrastructure as a Service
IaaSP	Infrastructure as a Service Provider
IoT	Internet of Things
ISS	Information Society Services
ISSPs	Information Society Services Provider
IT	Information Technology
MAC	Mandatory Access Control
P2P	Peer-to-Peer
PaaS	Platform as as a Service
PaaSP	Platform as as a Service Provider
PDCs	Personal Data Containers
PIS	Privacy Icons Software
RAC	Role Based Access Control
RCS	Remote Computing Service
SaaS	Software as a Service
SaaSP	Software as a Service Provider
Sub CSP	Sub Cloud Service Provider

LIST OF ABBREVIATIONS

A29WP	Article 29 Data Protection Working Party
ACLU	American Civil Liberties Union
ACM TMIS	ACM Transaction on Management Information Systems
ADR	Alternative Dispute Resolution
AFSJ	Area of Freedom, Security and Justice
AG	Attorney General
AJES	American Journal of Economics and Sociology
AJPS	American Journal of Public Science
Am Bus LJ	American Business Law Review
Am Econ Rev	American Economic Review
AM J Jurisprud	American Journal of Jurisprudence
Am Psychol	American Psychologist
AMR	Academy of Management Review
Annu Rev Sociol	Annual Review Sociology
AUBLR	American University Business Law Review
AUP	Acceptable Use Policy
Ave Maria L Rev	Ave Maria Law Review
BCRs	Binding Corporate Rules
B2C	Business to Consumer
Biochem J	Biochemical Journal
BTLJ	Berkeley Technology Law Journal
B U L Rev	Boston University Law Review
Bus L Rev	Business Law Review
Cal L Rev	California Law Review
CCR	Computer Communication Review
C2C	Consumer to Consumer
CIA	Central Intelligence Agency
CJCCJ	Canadian Journal of Criminology and Criminal Justice
CJEU	Court of Justice of the European Union (prior to December 2009, it was called the European Court of

	Justice (ECJ))
CLS Rev	Computer Law Security Review
CML Rev	Common Market Law Review
CoE	Council of Europe
CommLaw Conspectus	Journal of Communications Laws and Technology Policy
CUP	Cambridge University Press
DePaul Bus & Com LJ	Depaul Business & Commercial Law Journal
DNI	Director of National Intelligence
DoC	Department of Commerce
DOJ	Department of Justice
DOT	Department of Transportation
DP	Data Protection
DPA	Data Protection Authority
DPC	Data Protection Commissioner
DPD	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
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DuD	Datenschutz und Datensicherheit
Duke L & Tech Rev	Duke Law and Technology Review
DSSs	Decision Support Systems
EC	European Commission
ECD	E-Commerce Directive 2000
ECHRs	European Convention on Human Rights
ECPA	Electronic Communications Privacy Act of 1986
EDPS	European Data Protection Supervisory
EDI L Rev	Electronic Communication Law Review
EEA	European Economic Area

EEL	Transactions on Emerging Telecommunications Technologies
EHRLR	European Human Rights Law Review
EJLT	European Journal of Law and Technology
Emory LJ	Emory Law Journal
ENISA	European Network and Information Security Agency
EU	European Union
FBI	Federal Bureau of Investigation
Fed Cir B J	Federal Circuit Bar Journal
FGCS	Future Generation Computer System
FISA	Foreign Intelligence Surveillance Act of 1978
FISAA	Foreign Intelligence Surveillance Amendment Act of 2008
FISC	Foreign Intelligence Surveillance Court
FTC	Federal Trade Commission
FTC Act	Federal Trade Commission Act of 1914
GCHQ	Government Communication Headquarthers
GDPR	Regulations on of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation)
Geo L J	Georgetown Law Journal
Har L Rev	Harvard Law Review
HHRJ	Harvard Human Rights Journal
HLJ	Hastings Law Journal
Hous J Int'l L	Houston Journal of International Law
ICT Law	Information & Communications Technology Law
IDC	International Data Corporation
Idn L J	Indiana Law Journal
IDPL	International Data Privacy Law

IJACSA	International Journal of Advanced Computer Science and Applications
IJACT	International Journal of Advancements in Computing Technology
IJAEGT	International Journal of Advanced Engineering and Global Technology
IJARCET	International Journal of Advanced Research in Computer and Engineering & Technology
IJARET	International Journal of Advanced Research in Engineering & Technology
IJAST	International Journal of Advanced Science and Technology
IJBMS	International Journal of Business and Management
IJCAT	International Journal of Computer Applications in Technology
IJCCSA	International Journal on Cloud Computing: Services and Architecture
IJCNIS	International Journal of Computer Network and Information Security
IJDCF	International Journal of Digital Crime and Forensics
IJEME	International Journal of Education and Management
IJICT	International Journal of Information & Computation Technology
IJIS	International Journal of Information Security
IJITBM	International Journal of Information Technology and Business Management
IJLIT	International Journal of Law and Information Technology
IMCS	Information Management and Computer Security
Inform Manage	Information and Management
IP	Intellectual Property
IRLCT	International Review of Law Computers & Technology

JAMS	Journal of Academy of Marketing Science
J Appl Res Technol	Journal of Applied Research and Technology
JBEM	Journal of Broadcasting and Electronic Media
J Bus Ethics	Journal of Business Ethics
J Bus P	Journal of Business Perspective
JCA	Journal of Consumer Affairs
JCC	Journal of Computer and Communications
JCER	Journal of Contemporary European Research
JCLC	Journal of Criminal Law and Criminology
JCR	Journal of Conflict Resolution
JCSIT	Journal of Computer Science and Information Technology
JCSS	Journal of Computing and System Sciences
JDR	Ohio State Journal on Dispute Resolution
JEEA	Journal of the European Economic Association
JERML	Journal of Electronic Resources in Medical Libraries
JICE	Journal of International Commerce and Economics
J Internet L	Journal of Internet Law
JIPITEC	Journal of Intellectual Property, Information Technology and Electronic Commerce Law
JHA	Justice and Home Affairs
JIS	Journal of Information System
JISA	Journal of Internet Service and Applications
JITIM	Journal of International Technology and Information Management
JLER	Journal of Law and Economic Regulation
JM	Journal of Marketing
J Marshall J Computer & Info L	John Marshall Journal of Computer and Information Law
J Marshall J Info Tech & Privacy L	John Marshall Journal of Information Technology and Privacy Law
JMIR	Journal of Medical Internet Research
JNCA	Journal of Network and Communication Applications

JoCCASA	Journal of Cloud Computing: Advances, Systems and Applications
JoSS	Journal of Service Science Research
JOT	Journal of Object Technology
J Pers Soc Psychol	Journal of Personality and Social Psychology
JTLP	Journal of Technology Law and Policy
Law & Contemp Prob	Law and Contemporary Problems Journal
LEAs	Law Enforcement Agencies
LOR	Letter of Request
MD Law Rev	Maryland Law Review
Minn L Rev	Minnesota Law Review
MLATs	Mutual Legal Assistance Treaties
MLR	Modern Law Review
Monash Law Rev	Monash Law Review
MSBA	Maryland State Bar Association
MULR	Melbourne University Law Review
NGOs	Non Government Organisations
NIAs	National Intelligence Agencies
NJECL	New Journal of European Criminal Law
NSA	National Security Agency
OECD	Organisation for Economic Cooperation and Development
ODR	Online Dispute Resolution
OJEU	Official Journal of the European Union
OUP	Oxford University Press
PCJDPP	Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

PCLOB	Privacy and Civil Liberties Oversight Board
PDPJ	Privacy and Data Protection Journal
PE	Procedia Engineering
Pers Ubiquit Comput	Personal and Ubiquitous Computing
PL&B Inter Report	Privacy Laws & Business International Report
Priv LB	Privacy Law Bulletin
Procedia Comput Sci	Procedia Computer Science
Procedia Soc Behav Sci	Procedia Social and Behavioral Sciences
PSLR	Privacy and Security Law Report
QJEC	Quarterly Journal of Electronic Commerce
Q J Econ	Quarterly Journal of Economics
Res Organ Behav	Research Organisation Behavior
SCA	Stored Communication Act of 1986
SCCs	Standard Contractual Clauses
Sci Eng Ethics	Science and Engineering Ethics
Seton Hall L Rev	Seton Hall Law Review
SJIL	Standard Journal of International Law
SLA	Service Level Agreement
SMEs	Small and Medium Size Enterprises
Soc Networks	Social Networks Journal
Surveill Soc	Surveillance and Society
STIP	Scientific and Technical Information Processing
TEU	Treaty on the European Union
TFEU	Treaty on the Functioning of the European Union
TMO	Trustmark Organisation
ToS	Terms of Service
UALR LAW REVIEW	University of Arkansas at Little Rock Law Review
UCTD	Unfair Contract Terms Directive
UDHR	Universal Declaration of Human Rights
U Pa L Rev	University of Pennsylvania Law Review
US	United States
USDC	US Department of Commerce

VandJTransnatlL	Vanderbilt Journal of Transnational Law
Wash & Lee L Rev	Washington and Lee Law Review
Wm. Mitchell L. Rev	William Mitchell Law Review
WWPJ	Working Party on Police and Justice
YLJ Forum	Yale Law Journal Forum

INTRODUCTION

1. BACKGROUND

Cloud computing has become a popular way to offer Information Technology (IT) resources over the Internet. There are many kinds of cloud services offered to users, ranging from simply providing outsourced storage to the full external provision of hardware infrastructure.[1] Given the range of benefits promised by cloud services, such as lower costs, on-demand self-service, broad network access and rapid elasticity, cloud computing is increasingly used by many users, across the private and public sectors.

While many users enjoy using various types of cloud services, some hesitate to adopt them because their trust has been affected by the risks posed by cloud computing relating to many issues, e.g. loss of control over data, privacy and security.[2] Especially after the revelations of the United States (US) mass surveillance programme and the Cambridge Analytica data breach scandal, surveys have shown that some cloud users hesitate to entrust their data to cloud service providers (CSPs), especially to CSPs controlled from the US or which have servers located within the US.[3] All these scandals may yet prove to be a tipping point in how willing users are to place their trust in cloud computing.

Trust in cloud computing, which is seen as a critical factor enabling cloud users to be sufficiently confident to neglect such outcomes in exchange for benefiting from its advantages, has gained wide recognition as a key factor in the uptake of cloud computing, where there is a high possibility of an unsatisfactory outcome.[4] Trust in

---

[1] See more details in Chapter 1.

[2] See generally Siani Pearson and Azzedine Benameur, *Privacy, Security and Trust Issues Arising from Cloud Computing* (The 2nd International Conference on Cloud Computing 2010, Indiana, USA 2010).

[3] Charles Authur, 'Fears Over NSA Surveillance Revelations Endanger US Cloud Computing Industry' The Guardian, 8 August 2013 <http://www.theguardian.com/world/2013/aug/08/nsa-revelations-fears-cloud-computing> accessed 1 July 2017; Binns, A., 'Cambridge Analytica Scandal: Facebook's User Engagement and Trust Decline' (*28 March 2018*) <http://theconversation.com/cambridge-analytica-scandal-facebooks-user-engagement-and-trust-decline-93814> accessed 1 June 2018.

[4] See generally Felix Meixner and Ricardo Buettner, *Trust as an Integral Part for Success of Cloud Computing* (ICIW 2012 : The Seventh International Conference on Internet and Web Applications and Services 2012).

cloud computing does seem to be affected by the legal problems with Data Protection (DP), which result from a mismatch between DP laws and cloud technology.

As cloud computing has the potential to be a major driver for economic development, especially in developing countries – and it offers cheap services and an innovative ranges of services to individuals and Small and Medium Size Enterprises (SMEs) – a lack of user trust in cloud computing has been attracting widespread attention as it affects not only CSPs and cloud users, but also societies within the EU and potentially globally.[5]

2. REASONS TO STUDY

This thesis studies how user trust in cloud computing is affected by legal problems relating to DP in the cloud. In particular, it focuses on problems arising from fears over privacy and DP. It looks at two key legal problems; (1) the problems regarding the application of the EU (European Union) DP law to the processing of personal data in cloud computing; and (2) the problems regarding the EU and US legal frameworks governing access to personal data held in cloud computing by law enforcement agencies (LEAs) and national intelligence agencies (NIAs). This area is worthy of study for at least three reasons.

First, there is insufficient legal literature on the explored area due to the fact that the issue of trust in cloud computing is usually explored in a technological context, it has been little explored in a legal context. Second, the two key legal problems identified have been receiving special attention in the EU as a major concern within the reform process of EU DP law, following the revelations of mass surveillance conducted by the US government in 2013. As the two legal problems relating to DP in the cloud give rise to legal uncertainties, which then pose risks to the privacy of cloud users, these problems could potentially prevent users from placing trust in cloud computing and thus adopting it. Therefore, resolving the legal problems relating to DP in the cloud that could potentially lead to a lack of user trust in cloud computing, and at the same time making cloud computing trustworthy, is thus an urgent task in order to facilitate its commercial

[5] Commission, *Towards a Thriving Data-Driven Economy* (Brussels, 272014 COM(2014) 442 final).

and social benefits.

Lastly, this thesis will provide a clear understanding of what can make cloud computing trustworthy. This can help CSPs and legislators to develop appropriate approaches to build user trust in cloud computing, especially in my home country of Thailand, which is the funder of my study, as well as in other developing countries, which (1) do not yet have a strong history of cloud adoption or (2) are using or potentially supplying cloud services and still have no appropriate approach to ensure that CSPs will provide trustworthy services. Moreover, this thesis will provide useful information which will enable cloud users to consider which CSPs they should entrust with their personal data.

3. RESEARCH QUESTIONS

How is user trust in cloud computing affected by legal problems relating to safeguarding data privacy and how can we build user trust in cloud computing where it is damaged by these problems?

4. RESEARCH QUESTION STRUCTURE

In order to answer the main research question, the following sub-questions will need to be addressed:

A. What is cloud computing?

A.1 When was cloud computing first used?

A.2 How is cloud computing perceived by various scholars?

A.3 What are the characteristics of cloud computing?

A.4 How many kinds of cloud services are offered to users?

A.5 What are the benefits of cloud computing?

A.6 What are the drawbacks of cloud computing in terms of technical issues?

B. What are the key legal problems in cloud computing which might affect user trust in it?

C. What does trust mean in the context of cloud computing and why is it important?

C.1 How is trust perceived by different disciplines?

C.2 What are the key definitions of trust in cloud computing?

C.3 Do individuals and SMEs trust cloud computing?

C.4 What are the criteria for creating trust in cloud computing?

D. What are the legal problems affecting trust in cloud computing that emerge from EU DP law?

D.1 What are the EU legal frameworks governing the processing of personal data in the cloud?

D.2 What are the legal problems emerging from the application of Data Protection Directive 95/46/EC(DPD) in relation to the processing of personal data in the cloud?

D.3 How effectively does the General Data Protection Regulation (GDPR) address the problems surrounding applying the DPD in the context of cloud computing?

E. What are the legal problems affecting trust in cloud computing that arose out of the Snowden revelations about covert state surveillance of cloud users?

E.1 Which international multilateral or bilateral legal frameworks protect data subjects against interference with their privacy and private data by the State?

E.2 What are EU and US legal frameworks regarding access to personal data held in cloud computing for preserving privacy rights of individuals in the context of law enforcement and national security?

E.3 How effective were the US legal frameworks that were in operation up to the Snowden revelations, and the subsequent Schrems case, in providing EU cloud users with sufficient privacy protection to meet their expectations – and if not, why not?

E.4 How effectively do the legal frameworks proposed subsequent to the Snowden revelations by the US and EU address the problems affecting trust that arose out of those revelations?

F. What are the possible approaches for building user trust in cloud computing

where it is damaged by the two legal problems relating to DP?

5. LIMITS TO AND CONSTRAINTS ON THE THESIS

The scope of this thesis has certain limitations. First, this thesis will focus on trust as it could be used to rationalise people's decisions in a situation where there is an *incomplete evidence.* The concept of trust is different from the concept of confidence which always rests upon knowledge and a certain amount of evidence and the concept of faith which comes into play where there is *no evidence.*

Second, this thesis will not concentrate on trust of all cloud users, only on trust of EU individuals and SMEs. This is because trust plays quite a critical role for the use of cloud computing by individuals and SMEs, rather than larger companies. Larger companies will use cloud services if it saves them money and does not pose legal risks. And since they can pay for various types of insurance, they do not need to trust cloud computing. On the other hand, both individuals and SMEs normally have emotional reactions. Individuals are quite concerned about privacy risks brought about by cloud services. SMEs also have to consider how individuals feel when they offer services to them. In addition, individuals and SMEs generally do not have their own computing resources and they normally cannot afford insurances. Due to the fact that cloud computing could pose a number of risks and uncertainties to cloud users, individuals and SMEs may feel reluctant to adopt cloud services. If they do not use cloud services, in the end they will fail, with negative economic consequences. Individuals and SMEs will have to trust cloud computing by exposing themselves to its risks and uncertainties to take advantage of it.

Accordingly, it is worth considering how the trust of individuals and SMEs in cloud computing is affected by the legal problems relating to DP in the cloud in order to identify potential approaches to enable individuals and SMEs to place their trust in cloud computing and at the same time provide an adequate level of protection for the data residing in the cloud. If individuals and SMEs can fully trust cloud computing, they will agree to pay for various services offered by various different companies who intend to adopt cloud services for running their businesses. This would probably facilitate the whole system of cloud computing adoption and could potentially lead to global

economic development.

Third, it is important to highlight that this thesis will only concentrate on the legal problems relating to DP in the cloud. This is because these problems have been receiving special attention from the public, especially after the revelations of the US government's mass surveillance in 2013, as this exacerbated users' concerns regarding privacy, which tends to make existing and potential cloud users feel reluctant to adopt cloud computing.[6] It should be noted that the DP problems arising from the collection of personal data by Internet of Things (IoT) sensors into the cloud are not considered in this thesis.

Fourth, this thesis will explore the issue of trust and the legal problems relating to DP from an EU perspective. When exploring how user trust in cloud computing is affected by legal problems regarding the application of DP law to cloud computing, this thesis concentrates on EU DP law, where the DPD and the GDPR are the main DP laws in the EU for preserving the privacy of individuals who entrust their data to CSPs.

In addition, when exploring how user trust in cloud computing is affected by legal problems regarding access to personal data held in the cloud by LEAs and NIAs, this thesis only focuses on the situation where the data of EU data subjects stored with US CSPs or in US-located data centres ("US-controlled cloud") have been accessed by US LEAs and NIAs. The Snowden revelations (only the case of US surveillance) in 2013 are analysed as a landmark case study, which raised concerns in the EU about privacy protection in the cloud. Therefore, only the EU and US legal frameworks governing access to personal data held in the cloud as regards preserving the privacy of data subjects in the context of law enforcement and national security will be explored to see what level of privacy protection these legal frameworks offer to EU data subjects.

Lastly, this thesis is based to a large extent on the disillusionment with cloud computing felt after the Snowden revelations. However, other fears have recently emerged around cloud computing, such as in the domain of social media in the wake of the Cambridge Analytica and Russian interference in elections scandals near the end of

[6] See generally Siani Pearson, 'Privacy, Security and Trust in Cloud Computing' in Siani Pearson and George Yee (eds), *Privacy and Security for Cloud Computing* (Springer 2013); Commission, *Special Eurobarometer 431 on Data Protection* (March 2015).

the writing-up period. The author has taken all these into account but this does not change the main focus on the Snowden revelations.

6. RESEARCH METHODOLOGY

The research methodology adopted in this thesis in order to provide answers to the research questions is a doctrinal one, which includes an analysis of:

(a) EU legal primary texts, drawing mainly on human rights, DP and access to personal data by LEAs and NIAs, and those of the US where relevant;

(b) decisions of judicial bodies, i.e. the Court of Justice of the European Union (CJEU) and National Courts;

(c) secondary sources, such as books, academic articles, reports and discussion papers;

(d) decisions and working papers of the European Commission (Commission);

(e) opinions of and recommendations by the Article 29 Data Protection Working Party (A29WP);

(f) empirical evidence from various sources relating to trust of individuals and SMEs in cloud computing and its adoption.

The study is desk-based. The author has not attempted to interview EU individuals and SMEs that have been using cloud services nor has the author sent questionnaires to them due to lacking the necessary resources to do so, the difficulties of identifying a suitably representative group of individuals and SMEs to interview/ question and the traditional low response rate to questionnaires sent out by students. The sources considered are limited to those consulted up to the end of July 2018.

7. ORIGINAL CONTRIBUTIONS

The existing literature has only studied the issue of trust in cloud computing from a technical perspective. Many technical scholars have tried to explore technical issues which lead to the death of trust in cloud computing, which then make users hesitate to adopt cloud services with a view to proposing a guidance for CSPs to make their

services trustworthy in order to attract people to adopt cloud services.[7] For example, in order to build user trust in cloud computing, Valentine and Enyinna suggested to apply the cryptographic computation protocols which support computation on cipher text to sensitive data uploaded to the cloud in order to avoid unauthorised access to the data, and also suggested that any application running in the cloud should not be allowed to directly decrypt the data.[8] Furthermore, Wu et al. aimed to increase user trust in cloud computing by proposing a trust evaluation model based on the D-S evidence theory and this model could be used to identify malicious entities, and to provide reliable information to correctly make security decisions for the system.[9]

Nevertheless, the technical issue is not the only factor that can weaken user trust in cloud computing. The legal problems could potentially make people refrain from placing their trust in cloud computing since the legal problems do pose privacy risks to cloud users.[10]

This situation leaves room for the author to study the issue of trust in cloud computing from a legal perspective. Although a few contributions to the legal literature were found that mention the issues of trust in cloud computing (which are always trust of big business rather than trust of individual and SMEs in cloud computing), the issues explored in this research have yet to be thoroughly examined.

The Centre for Commercial Law Studies at Queen Mary, University of London, conducted its multi-year Cloud Legal Research Project, which was started in October 2009 and was funded by Microsoft Corporation. This project explored the legal and regulatory problems in cloud computing at many areas and at the intersection of cloud computing and the IoT, including the DP problems resulting from the application of the

[7] The examples from the current literature which explore the issue of trust from a technical perspective are: Imad M. Abbadi and Muntaha Alawneh, 'A Framework for Establishing Trust in the Cloud ' (2012) 38 Computers and Electrical Engineering 1073;Imad M. Abbadi, 'A Framework for Establishing Trust in Cloud Provenance' (2013); Jingwei Huang and David M Nicol, 'Trust Mechanisms for Cloud Computing' (2013) 2 JoCCASA 1. See more details in chapter 2.

[8] Valentine UI and Enyinna OU, 'Building Trust and Confidentiality in Cloud Computing Distributed Data Storage' (2013) 6 West African Journal of Industrial & Academic Research 78.

[9] Wua X and others, 'A Trust Evaluation Model for Cloud Computing' (2013) 17 Procedia Computer Science 1170.

[10] Commission, *Unleashing the Potential of Cloud Computing in Europe* (Brussels, 2792012 COM(2012) 529 final) 8-9.

EU DP law in cloud computing and from access to personal data held in cloud computing by LEAs.[11] However, the issue of government surveillance was not explored in this project. And this research focused heavily on enhancing the trust of business users in cloud computing, so that the issue around trust of individual users was not discussed.

The Cloud Accountability Project (A4Cloud), was a collaborative project of various academic and industrial institutes, such as Tilburgh University, Hewlett-Packard Limited and a non-profit organisation, 'Cloud Security Alliance', run from October 2012 - March 2016.[12] This project focused heavily on the issue of accountability. It explored how to solve problems of ensuring trust in cloud computing by providing tools which are interdisciplinary and which include legal and regulatory, socio-economic and technical aspects that support the process of achieving accountability for CSPs, such as the Cloud Offering Advisory Tool (COAT), the Data Protection Impact Assessment Tool (DPIAT), the Data Track Tool (DTA) and the Data Protection Policies Tool (DPPT). However, the issue of government surveillance had been excluded from the scope of this project.

The scholars from the Cyberspace Law and Policy Centre, Faculty of Law, University of New South Wales have studied in 2013 the technical, legal and risk governance issues around data hosting and jurisdiction in cloud computing, including the issues regarding getting access to data held in cloud computing by governments.[13] This project focused primarily on the Australian jurisdiction, but it did touch on the relevant law and practices of the US. This project suggested to adopt specific policy for cloud data location and jurisdiction, including data practice that fulfil the relevant legal requirements. Nevertheless, the issues around user trust in cloud computing, e.g. how is

[11] The Cloud Legal Project by the Centre for Commercial Law Studies at Queen Mary, University of London, available at <http://www.cloudlegal.ccls.qmul.ac.uk> accessed 11 March 2018.
[12] The Cloud Accountability Project for Cloud, partly funded by the European Community's Seventh Framework Programme, available at < http://www.a4cloud.eu.> accessed 11 March 2018.
[13] The Data Sovereignty and the Cloud Report by the Cyberspace Law and Policy Centre, Faculty of Law, University of New South Wales, available at < http://www.cyberlawcentre.org/data_sovereignty/index.htm > accessed 20 March 2018.

user trust affected by such issues, the criteria for evaluating trust in cloud computing or how to build user trust in cloud computing, were not mentioned in this project.

Hence, the original contribution of this research lies in the fact that the issue of the trust of individuals and SMEs in cloud computing, which is discussed in a legal context relating to the specific two legal problems with DP, has not been thoroughly studied before. Moreover, this research is probably the only one to study the legal problems with DP in cloud computing through a study of the full process of the EU DP reform and the Snowden revelations.

8. Structure of the Thesis

Introduction

Chapter 1: Introduction to Cloud Computing addresses sub-research questions A and B by presenting an overview of cloud computing. There are seven sections in this chapter, including its history, definitions, characteristics, categories, benefits and disadvantages. Furthermore, the legal problems with cloud computing in connection with four main issues: DP, contracts, intellectual property, crime and forensics, are briefly explained in the last section.

Chapter 2: The Concept of Trust in Cloud Computing responds to sub-research question C by exploring the concept of trust in cloud computing. There are two sections in this chapter. Section one presents a description of trust from various different disciplines, namely, psychology, sociology, business and electronic commerce, by focusing on the issue of what creates trust, what breaks trust and how to build trust. Section two conducts an analysis of the concept of trust in cloud computing in relation to three main issues: (1) key definitions of trust in cloud computing; (2) whether individuals and SMEs trust cloud computing, which is based on empirical evidence from various sources; and (3) criteria for creating trust in cloud computing.

Chapter 3: Legal Problems Regarding the Application of the EU Data Protection Law in Cloud Computing seeks to address sub-research question D. There are two sections in this chapter. Section one explores the EU DP law, with an emphasis

on the DPD, governing the processing of personal data in the cloud. Section two discusses the legal problems affecting trust in cloud computing that emerge from the application of the DPD in the context of cloud computing, as well as an analysis of how effective the GDPR is in addressing these problems and potential solutions to those problems.

Chapter 4: Legal Problems Regarding the EU and US Legal Frameworks Governing Access to Personal Data Held in Cloud Computing by Law Enforcement and National Intelligence Agencies provides answers to sub-research question E. There are two sections in this chapter. Section one is separated into four parts to consider legal frameworks regarding access to personal data of EU data subjects held in the cloud for preserving privacy of individuals in the context of law enforcement and national security, including (1) international multilateral/ bilateral frameworks; (2) EU legal frameworks; (3) US legal frameworks; and (4) the EU-US Agreement. Section two is separated into three parts to (1) examine the defects in US legal instruments that lead to mass surveillance; (2) discuss whether the US legal frameworks, and the EU-US legal instruments for data transfer from the EU, which were in operation up to the Snowden revelations, and the subsequent *Schrems* case, offered EU cloud users sufficient privacy protection to meet their expectations; and (3) analyse whether the legal frameworks proposed subsequent to the Snowden revelations by the EU and US work satisfactorily to address the existing problems.

Chapter 5: Solutions to the Lack of User Trust in Cloud Computing engages with sub-research question F by seeking to propose possible approaches for enhancing user trust in cloud computing. This chapter proposes two main types of solutions, legal and non-legal, to the lack of trust in cloud computing. All these approaches aim to satisfy three criteria for creating trust in cloud computing by: (1) improving transparency and control; (2) enhancing accountability; and (3) increasing data security, in order to make users be more confident to ignore, more or less, the risks posed by cloud computing for the sake of taking advantages of cloud computing. Some observations when selecting each proposed approach are also discussed.

Conclusion draws together answers to all the research questions raised by this thesis.

CHAPTER 1

INTRODUCTION TO CLOUD COMPUTING

INTRODUCTION

Over the past few years, cloud computing has become the dominant model for providing Information Technology (IT) resources over the network. It enables users to store or process data on a cloud infrastructure rather than using their own local resources.[1] While many users are enjoying using cloud services nowadays, there remain some individuals and Small and Medium Sized Enterprises (SMEs) who are hesitant about adopting cloud computing, due to many potential risks it can impose, such as privacy risks.[2]

This chapter deals with Research Questions A: what is cloud computing? and Research Question B: what are the key legal problems in cloud computing which might affect user trust in it?

There are seven sections in this chapter. Following this introduction, the genesis and evolution of cloud computing are elucidated, in order to enable the reader to understand the underlying concept of cloud computing. Then, definitions of cloud computing proposed by different sectors, including IT, business and legal sectors, are presented in section two. Section three describes essential characteristics of cloud computing, followed by a description of the types of cloud computing categorised by the service model and the deployment model discussed in section four.

Following that, section five provides benefits offered by cloud computing. Then, section six raises some drawbacks of cloud computing, with an emphasis on the technical issues. Section seven briefly discusses legal problems in cloud computing, with regard to four main issues, including data protection (DP), contract, intellectual property, and crime and forensic. Finally, conclusions are drawn from various points raised in this chapter.

1. GENESIS AND EVOLUTION OF CLOUD COMPUTING

[1] Daryl C. Plummer and others, *Cloud Computing : Defining and Describing an Emerging Phenomenon* (Gartner,17 June 2008) 2.
[2] ENISA, *An SME Perspective on Cloud Computing : Survey* (June 2010).

The emergence of cloud computing has drawn the attention of a wide range of users, ranging from private to public sectors. To some, it was seen as a new technology within the entire IT world. To others, it was considered as the modernisation of previous technology, namely the time-sharing paradigm.[3] Due to the fact that the underlying concept of cloud computing is still based on existing technologies, such as Virtualisation, Web Service or Grid Computing, cloud computing is regarded as being an extension to the achievement of existing technologies, rather than a revolutionary step beyond current technologies.[4]

The most important type of technology considered as inspiring the invention of cloud computing is Grid Computing, which emerged in the 1990s.[5] The underlying concept of Grid Computing is 'the coordinated resource sharing and problem solving in dynamic, multi-institutional virtual organisations'.[6] Thus, many separate personal computers could be interconnected as a grid with a view to facilitating the scaling up of computing resources, with users having easy access to the resulting service via the Internet.[7] One example of Grid Computing is Peer-to-Peer (P2P) file sharing.[8]

In the 2000s, many industries tried to find the best approach for leveraging the latent processing power of such systems after discovering that their large IT purchases were being left idle and only fully utilised during the peak periods of requests.[9] This situation led to the invention of a new approach aimed at harnessing the distributing of resources by service providers, in order to meet the needs of each user and to enable users to pay according to their actual usage.[10] Ultimately, this concept was named as

---

[3] Winston Churchill, 'Cloud Computing Fundamentals' in Ronald L. Krutz and Russell Vines Dean (eds), *Cloud Security: A Comprehensive Guide to Secure Cloud Computing* (John Wiley & Sons 2011) 1.
[4] Omkhar Arasaratnam, 'Introduction to Cloud Computing' in Ben Halpart (ed), *Auditing Cloud Computing: A Security and Privacy Guide* (John Wiley & Sons 2011) 2.
[5] Richard Hill and others, *Guide to Cloud Computing: Principles and Practice* (Springer 2013) 6.
[6] Ian Foster and Carl Kesselman, 'Concepts and Architecture' in Ian Foster and Carl Kesselman (eds), *The Grid 2 : Blueprint for a New Computing Infrastructure* (Morgan Kaufmann Publishers 2004) 37.
[7] Hill and others (n5) 2.
[8] The concept of Peer to Peer (P2P) file sharing is to allow individual computer users (called Peers) in the same network to connect with each other and directly access files in the hardware of the other computer users. See Quang Hieu Vu, Mihai Lupu and Beng Chin Ooi, *Peer to Peer Computing : Principle and Application* (Springer 2010) 5.
[9] Arasaratnam (n4) 2.
[10] David Villegas and others, 'The Role of Grid Computing Technologies in Cloud Computing' in Borko Furht and Armando Escalante (eds), *Handbook of Cloud Computing* (Springer 2010) 185.

'Cloud Computing'.

The concept of cloud computing does, in fact, date back to the 1960s when it was predicted by John McCarthy, a computer professional at the Massachusetts Institute of Technology, that, in the future, computing resources might be delivered as a public utility.[11] The utility computing concept was then expanded by Douglas Parkhill in 1966.[12] He took the view that computing resources should be available as an unlimited supply and should be available everywhere through access to a network.[13] Following that, the concept of cloud computing developed and has now been around for some time in the form of Software as a Service (SaaS).[14] Among the first cloud services offered to the public were Webmail Services, such as Gmail, Hotmail and Yahoo.[15] These services shifted the ways of providing email from desktop applications to Internet-based applications offered by CSPs (cloud service providers).[16] The popularity of Webmail Services led to the advancement of other kinds of cloud services.[17] It can be seen that cloud computing is a growing field and is continuing to have an impact on many sectors, including individuals, businesses and public organisations.[18]

2. DEFINITIONS OF CLOUD COMPUTING

The term "cloud computing" was inspired by the cloud symbol that is often used as a metaphor for the Internet in flow charts.[19] It was first used as an umbrella term indicating an on-demand computing service offered by various providers, such as

[11] J McCarthy, 'Reminiscences on the History of Time Sharing' Stanford University <http://www-formal.stanford.edu/jmc/history/timesharing/timesharing.html> As cited in Hill and others (n5) 4.
[12] Douglas Parkhill, *The Challenge of Computing Utility* (Addison-Wesley Pub 1966) 33.
[13] Arasaratnam (n4) 1; Hill and others (n5) 4.
[14] Michael J. Kavis, *Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS)* (Wiley 2014) 7.
[15] David A Couillard, 'Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing' (2009) 93 Minn L Rev 2205, 2218.
[16] William Jeremy Robinson, 'Free at What Cost? Cloud Computing Privacy Under the Stored Communications Act ' (2010) 98 Geo L J 1195, 1203.
[17] ibid.
[18] ibid 1201.
[19] Zaigham Mahmood, 'Cloud Computing for Enterprise Architectures' in Zaigham Mahmood and Richard Hill (eds), *Cloud Computing for Enterprise Architectures* (Springer 2011) 3.

Amazon, Microsoft and Google.[20] Although cloud computing has become a popular service over the past few years, there are no formal definitions of cloud computing.[21] Moreover, the understanding of what cloud computing is remains in a state of uncertainty.[22] An exact definition of cloud computing still being a subject of debate.[23] This section provides definitions of cloud computing introduced by different sectors, as follows.

2.1 Definitions of Cloud Computing from IT Sector

Buyya et al. (2008) defined cloud computing as

> a type of parallel and distributed system consisting of a collection of inter-connected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resources based on service-level agreements established through negotiation between the service provider and consumers.[24]

Forster et al. (2008) viewed cloud computing as

> a large-scale distributed computing paradigm that is driven by economies of scale, in which a pool of abstracted, virtualized, dynamically-scalable, managed computing power, storage, platforms, and services are delivered on demand to external users over the Internet.[25]

Plummer et al. (2008) defined cloud computing as

> a style of computing where scalable and elastic IT capabilities are provided

[20] William Voorsluys, James Broberg and Rajkumar Buyya, 'Introduction to Cloud Computing' in Rajkumar Buyya, James Broberg and Andrzej Goscinski (eds), *Cloud Computing: Principle and Paradigms* (John Wiley & Sons 2011) 3.
[21] Hai Jin and others, 'Cloud Types and Services' in Borko Furht and Escalante Armando (eds), *Handbook of Cloud Computing* (Springer 2010) 335.
[22] Samson Yoseph Esayas, 'A Walk in to The Cloud and Cloudy It Remains: The Challenges and Prospects of 'Processing' and 'Transferring' Personal Data ' (2012) 28 CLS Rev 662, 662.
[23] Primavera De Filippi and Smari McCarthy, 'Cloud Computing: Centralization and Data Sovereignty' (2012) 3 EJLT 1, 2.
[24] Rajkumar Buyya and others, 'Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility' (2009) 25 FGCS 599, 601.
[25] Ian Foster and others, *Cloud Computing and Grid Computing 360-Degree Compared* (Grid Computing Environments Workshop (GCE) 12-16 November, 2008),1

as a service to multiple users using Internet technologies.[26]

Armbrust et al. (2009) described cloud computing as

> the illusion of infinite computing resources available on demand, the elimination of up-front commitments by cloud users, and the ability to pay for use of computing resources on a short- term basis as needed.[27]

Mell and Grance (2009) defined cloud computing as

> 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.[28]

2.2 Definitions of Cloud Computing from Business Sector

Microsoft (2010) viewed that

> cloud computing represents a transformation of the industry in which we and our partners work to deliver *IT as a Service*. This transformation will let you focus on your business, not on running infrastructure. It will also let you create better applications, then deploy those applications wherever makes the most sense: in your own data center, at a regional service provider, or in our global cloud. In short, IT as a Service will let you deliver more business value.[29]

Intel (2013) opined that

---

[26] Plummer and others (n1) 3.
[27] Michael Armbrust and others, *Above the Clouds : A Berkeley View of Cloud Computing* (Technical Report No UCB/EECS-2009-28 (10 February 2009))1.
[28] Peter Mell and Timothy Grance, *The NIST Definition of Cloud Computing* (Recommendation of the National Institute of Standards and Technology, 2011) 2.
[29] Microsoft, 'IT as a Service : Transforming IT with the Windows Azure Platform' November 2010 <http://download.microsoft.com/download/C/D/A/CDAE9B95-F03A-4C80-AC07-3B03AF42817B/ITasaService-v1.pdf> accessed 11 July 2017 , 1.

> cloud computing is an evolution of IT services delivery that offers a path to optimized use and rapid deployment of resources through systems that solutions are more efficient and scalable, while providing much greater levels of automation.[30]

2.3 Definitions of Cloud Computing from Legal Sector

Hon and Millard (2013) defined cloud computing as

> a way of delivering computing resources as a utility service via a network, typically the Internet, scalable up and down according to user requirements.[31]

Leenes (2013) described that

> cloud computing encompasses a multitude of different service and deployment models. The most important is the fact that the provider's computing resources are pooled to serve multiple consumers using a multi-tenant model.[32]

Schwartz (2013) defined cloud computing as

> the locating of computing resources on the Internet in a fashion that makes them highly dynamic and scalable. This kind of distributed computing environment can quickly expand to handle a greater system load or take on new tasks. Cloud computing thereby permits dramatic flexibility in processing decisions—on a global basis.[33]

It is clearly seen that scholars from different sectors have proposed their own cloud computing definition based on their focus. The significant difference among the

---

[30] Intel, 'Intel's Vision of Open Cloud Computing' August 2013 <http://www.intel.la/content/dam/www/public/us/en/documents/white-papers/open-cloud-computing-vision-paper.pdf> accessed 11 July 2017, 3.
[31] W Kuan Hon and Christopher Millard, 'Cloud Technologies and Services' in Christopher Millard (ed), *Cloud Computing Law* (Oxford University Press 2013) 3.
[32] Ronald Leenes, *Who Controls the Cloud?* (6th IDP Conference Cloud Computing: Law and Politics in The Cloud 2010) 6.
[33] Paul M. Schwartz, 'Information Privacy in the Cloud ' (2013) 161 U Pa L Rev 1623, 1624.

definitions is that each one concentrates on different aspects of cloud computing. On one hand, in the IT sector, most of the cloud definitions mention several technologies that cloud computing draws on, such as Virtualisation, Distributed Systems, Abstraction or Pooling Resources. IT scholars have tried to define cloud computing by providing technical information about the nature, or functioning, of cloud computing.

On the other hand, scholars from the business sector, such as Microsoft and Intel, did not seem to pay attention to providing an exact description of cloud computing. They merely described it as a way to attract users to adopt their own cloud services by referring to the cloud services they market.

The definitions of cloud computing put forward by legal scholars have been relatively few, due to it recently being discovered that cloud computing has created some challenges for law enforcement, which still cannot be properly dealt with by existing legal frameworks.[34] Many legal scholars have, consequently, started to investigate cloud computing and describe it in their own way in aiming to raise the level of understanding of cloud computing among legal scholars. The Cloud Legal Research Project carried out by legal scholars from the Centre for Commercial Law Studies at Queen Mary, University of London is the leading example of such research.[35] In summary, the distinctive characteristic of the cloud computing definition presented by legal scholars is that they focus on the specific features of cloud computing that create difficulties for applying the law in the context of cloud computing, such as pooled resources and location-independence.

	Buyya et al.	**Forster et al.**	**Plummer et al.**	**Armbrust et al.**	**Briscoe and Marinos**	**Mell and Grance**	**IBM**	**Microsoft**	**Intel**	**Dell**	**Hon and Millard**	**Leenes**	**Schwartz**
Distribution													
Virtualization													

[34] Anthony Gray, 'Conflict of Laws and the Cloud' (2013) 29 CLS Rev 58, 58.
[35] Cloud Legal Research Project (CLP) was carried out with a view to engaging with various legal issues brought about by cloud computing. See <http://www.cloudlegal.ccls.qmul.ac.uk> accessed 14 February 2018.

Scalability	■	■	■	■	■	■			■		■		■
Ubiquitous Network	■	■	■		■	■	■	■		■	■		■
Pooled Resources		■				■				■		■	
Abstraction		■			■								
On-Demand Services		■		■		■				■	■		
Pay-Per-Use Services				■									
Fast Deployment						■			■	■	■		■
Multi-Tenancy			■									■	
Customers' own data centre								■					
Automation									■				
IT Service delivery					■		■		■		■	■	■
Utility Computing				■							■		

Table 1. Characteristics of Cloud Computing

According to this table, although different sectors have proposed their own definitions based on their focus, there are some common conceptualisations of cloud computing that are drawn on by the majority of these definitions, such as ubiquitous network, scalability, pooled resources and on-demand services. The author of this thesis aims to propose the key concept of cloud computing as follows:

> *Cloud computing is a paradigm for delivering IT capabilities over the Internet. It provides many kinds of services, ranging from mere software to the whole infrastructure in different models. Cloud resources are pooled together, so that cloud services are scalable and can be rapidly provisioned. It allows users to monitor and customise their own resources as needed. Cloud users will then be billed on the basis of their measured usage*.

3. CHARACTERISTICS OF CLOUD COMPUTING

3.1 On Demand Self-Service

Cloud computing allow users to make use of such IT capabilities as storage and computation as needed.[36] Cloud users can customise their own resources without having to wait for CSPs to fulfill their demands.[37] This means that IT resources are scalable and instantly available to users over the network.[38] There is no human interaction between cloud users and CSPs in this situation.

3.2 Ubiquitous Network Access

Cloud services are available over the Internet and can be accessed through standard devices, such as smart phones, tablets and laptops.[39] Therefore, cloud users can easily gain access to cloud services at any time and from anywhere wherever an adequate Internet Protocol network is available.[40]

3.3 Pooling of Resources

Cloud computing resources are pooled together into a large resource that enables cloud users to leverage the service to meet their demands.[41] The pooled resource can be provided to many users to save the cost of CSPs.[42] Resources that are not being used by one user will not be left idle, as they could be used by others.[43] Cloud users may have no knowledge of the exact location of the service being offered by CSPs.[44]

3.4 Pay-Per-Use Service

---

[36] Mell and Grance (n28) 2.
[37] Navin Sabharwal, *Cloud Capacity Management* (Apress 2013) 2.
[38] Eric Bauer and Randee Adams, *Reliability and Availability of Cloud Computing* (John Wiley & Sons 2012) 4; Borko Furht, 'Cloud Computing Fundamentals' in Borko Furht and Armando Escalante (eds), *Handbook of Cloud Computing* (Springer 2010) 11.
[39] Mell and Grance (n28) 2.
[40] Bauer and Adams (n38) 5.
[41] Hill and others (n5) 9.
[42] Bauer and Adams (n38) 5.
[43] Derrick Rountree and Ileana Castrillo, *The Basics of Cloud Computing: Understanding the Fundamentals of Cloud Computing in Theory and Practice* (Syngress 2013) 5.
[44] Mell and Grance (n28) 2.

Cloud computing is provided on the basis of a pay-per-use model.[45] The resources can be measured by using various metrics, such as time used or data used, and then this measured usage can be promptly reported to users.[46] Cloud users will be billed according to their actual usage, rather than being charged a fixed price.[47]

3.5 Rapid Elasticity

Cloud computing allows users to rapidly scale the capabilities up or down as needed.[48] Cloud capabilities are available to users as a large dynamic resource that can be automatically allocated and can be provisioned at any time with acceptable service quality.[49] The rapid elasticity of cloud computing enables cloud users to save on costs, as the capabilities can be increased during peak times, as well as decreased during off-peak times.[50]

4. TYPES OF CLOUD COMPUTING

4.1 Categorised by Service Model

4.1.1 Software as a Service (SaaS) provides users with the provider's application, which runs on cloud infrastructure, through the Internet as a Web-based service.[51] Cloud users cannot control or manage an underlying cloud infrastructure, such as servers, storage, operating system and network, except for a limited administrative application setting.[52] Software as a Service Provider (SaaSP) mainly takes responsibility for security provisions.[53] Examples of SaaS are Facebook and Dropbox.

4.1.2 Platform as a Service (PaaS) functions on top of infrastructure as a service[54] and provides users with the tools required to develop and deploy an application

---

[45] ibid 2.
[46] Rountree and Castrillo (n43) 5; Voorsluys, Broberg and Buyya (n20) 16.
[47] Bauer and Adams (n38) 6.
[48] Mell and Grance (n28) 2.
[49] Churchill (n3) 11.
[50] Bauer and Adams (n38) 6.
[51] Rajkumar Buyya, Christian Vecchiola and S. Thamarai Selvi, *Mastering Cloud Computing Foundations and Applications Programming* (Elsevier 2013) 121.
[52] Wayne Jansen and Timothy Grance, *Guidelines on Security and Privacy in Public Cloud Computing* (Report of the National Institute of Standards and Technology, January 2011) 3-4.
[53] ibid 3.
[54] Kavis (n14) 15.

on cloud infrastructure.[55] The application might be a user-created or acquired application produced by using the programming, tools and services supported by CSP.[56] Cloud users can have control over the applications and the application environment settings of the platform, but cannot manage the underlying cloud infrastructure.[57] Both the Platform as a Service Providers (PaaSP) and cloud users take responsibility for the security provisions.[58] The Google App Engine (GAE) and Microsoft Window Azure are examples of PaaS.

4.1.3 Infrastructure as a Service (IaaS) provides users with the means to run their software with different kinds of infrastructure resources, including servers, software and networks.[59] While Infrastructure as a Service Provider (IaaSP) operates an entire infrastructure and data centres, cloud users are allowed to have full control over all aspects of the deployment, including operating systems, web services, applications and programming languages.[60] Cloud users mainly take responsibility for the security provisions beyond the basic infrastructure.[61] Examples of IaaS are GoGrid and Amazon Elastic Cloud (EC2).

[55] Gautam Shroff, *Enterprise Cloud Computing : Technology, Architecture, Applications* (Cambridge University Press 2013) 56.
[56] Mell and Grance (n28) 2-3.
[57] Jansen and Grance (n52) 4.
[58] ibid 3.
[59] Arasaratnam (n4) 5.
[60] Hill and others (n5) 105.
[61] Jansen and Grance (n52) 4.

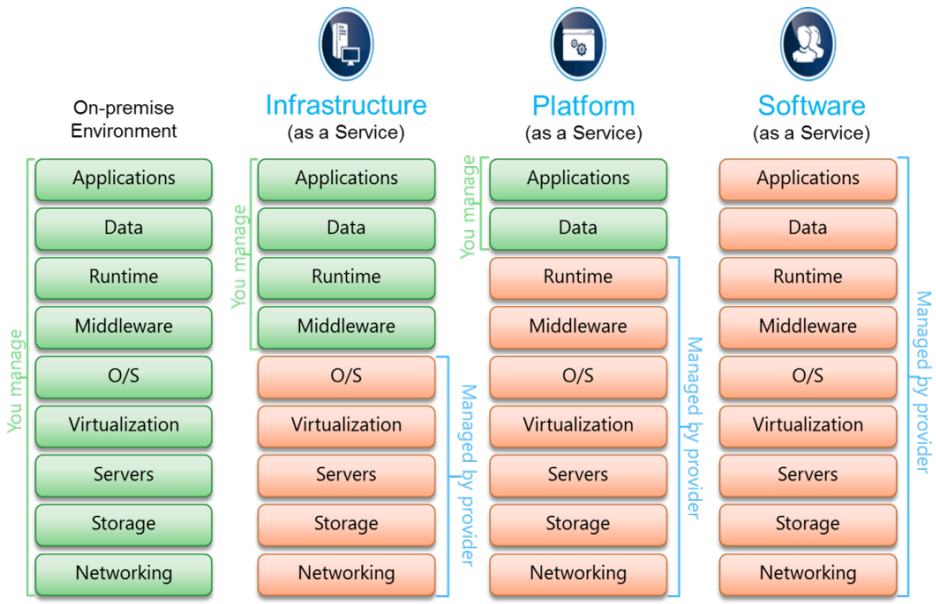

Figure 1. Three Service Models of Cloud Computing [62]

It can clearly be seen that the significant difference among the different kinds of CSP is the ability to control each component of the cloud infrastructure, which is the main factor considered when determining who will be responsible for the occurrence of any loss or damage to the data held in the cloud computing. For this reason, it is vital for cloud users to know what kinds of CSPs are delivering services to them.

As a variety of different actors involved in cloud services will be mentioned in relation to many issues discussed in this thesis, this section provides the names and clear descriptions of the actors that will be involved in the different kinds of cloud services, as follows.

(a) Cloud Service Provider (CSP) is the name generally allocated to who is providing any kind of cloud service to cloud users.

(b) Primary Cloud Service Provider (Primary CSP) is the CSP with whom cloud users have a contract.

[62] SaSS, PaSS and IaSS Making Cloud Computing Less Cloudy.
See < http://cioresearchcenter.com/2010/12/107/ > accessed 15 February 2017.

(c) Sub – Cloud Service Provider (Sub-CSP) is a CSP who does not have a direct contractual relationship with cloud users.

(d) Software as a Service Provider (SaaSP) provides an application to cloud users. All components of the cloud infrastructure, such as applications, servers and networks, are operated solely by the SaaSP. Even if customisation of the application may be allowed in some cases, cloud users still have to ask the SaaSP to make a change for them, rather than making it by themselves.[63]

(e) Platform as a Service Provider (PaaSP) provides a platform to users. This platform includes all of the facilities for developing, integrating and testing applications, enabling users to build and run their own applications.[64] While cloud users install, maintain and monitor their own applications, the PaaSP is responsible for ensuring that the operating system is ready for users to deploy the applications.[65] Therefore, all of the components of cloud infrastructure under the platform level are controlled mainly by the PaaSP.

(f) Infrastructure as a Service Provider (IaaSP) provides the virtual infrastructure to users. Most of the cloud infrastructure, for example, its computing powers, database and operating system, are controlled by cloud users. However, the physical hardware, storage and networking are still located in the data centre of the IaaSP, with cloud users having full access to them.[66] Consequently, the IaaSP is still responsible for the lowest layer of cloud infrastructure, including server, storage and networking.

(g) Cloud User refers to anyone who adopts a cloud service. When using different kinds of cloud service, each cloud user can control each component of the cloud infrastructure differently.

4.2 Categorised by Deployment Model

4.2.1 Private Cloud is operated solely for a single organisational unit.[67] This

[63] Rountree and Castrillo (n43) 51.
[64] ibid 62.
[65] ibid 64.
[66] Hill and others (n5) 10.
[67] Christian Baun and others, *Cloud Computing: Web-Based Dynamic IT Services* (Springer 2011) 15.

model may be controlled within the organisation or by third parties, and might be located within the organisation's facilities or outsourced.[68] Normally, this model is adopted by organisations aiming to maintain their data in a more controlled and safe environment.[69] Examples of private cloud are Amazon Virtual Private Cloud and Enomaly Cloud Service Provider Edition.

4.2.2 Community Cloud is operated for a specific community of users who share similar concerns, such as mission, policy and security requirements.[70] The users could be individuals, businesses or public organisations having the same purpose for using cloud services.[71] It may also be owned and controlled by one or more organisations in the community[72] It could be located within organisations' facilities or may be outsourced.[73] The G-Cloud of the UK government is an example of a community cloud.

4.2.3 Public Cloud is the first expression of cloud computing to be implemented.[74] This model is available for the general public and is provided by third parties, but controlled by a CSP.[75] The CSP is in charge of the installation, provision and maintenance.[76] A public cloud is located outside organisations' own facilities.[77] Examples are Google Apps and Microsoft Azure.

4.2.4 Hybrid Cloud is a combination of many types of cloud deployment models (Private, Community or Public).[78] Each type of model is bound by standardised technology that makes the data and applications portable.[79] This model combines external capacity with on-premises resources.[80] Examples are Carpathia and Skytap.

---

[68] Mell and Grance (n28) 3.
[69] Jin and others (n21) 338.
[70] Mell and Grance (n28) 3.
[71] Buyya, Vecchiola and Selvi (n51) 131.
[72] Hill and others (n5) 11-12.
[73] Mell and Grance (n28) 3.
[74] Rountree and Castrillo (n43) 36.
[75] Hill and others (n5) 11.
[76] Mahmood (n19) 6.
[77] Mell and Grance (n28) 3.
[78] ibid 4.
[79] ibid.
[80] Mahmood (n19) 6.

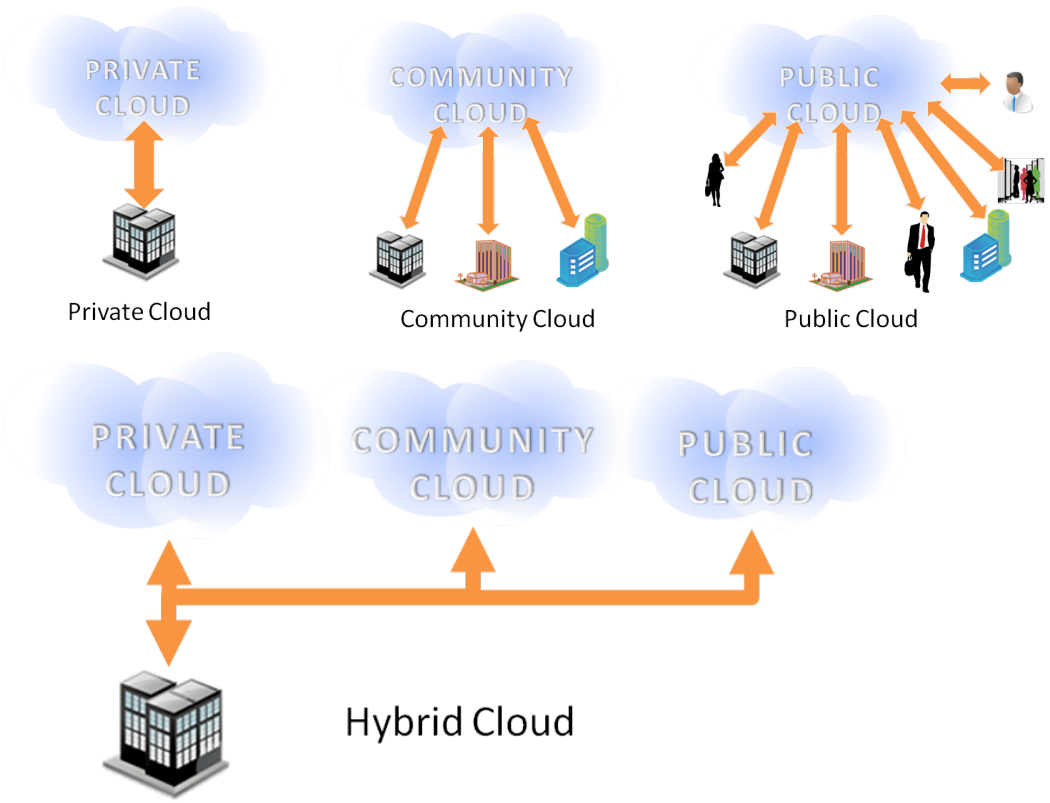

Figure 2. Four Deployment Models of Cloud Computing [81]

5. BENEFITS OF CLOUD COMPUTING

5.1 Reduce Cost

Cloud users are not required to pay for hardware, software and operating fees, such as license fees, maintenance fees or professional service fees, as the CSP provides all of these to cloud users.[82] As for CSPs, they are not required to invest heavily in infrastructure to provide service to many users, as cloud infrastructures are pooled together to serve multiple users. Furthermore, there is no need for them to employ many IT administrators to deploy their services to users, as cloud users, themselves, manage

[81] Cloud Computing – Deployment Models. <http://howcrmworks.com/tag/cloud-computing/> accessed 1 February 2014.
[82] Jared A. Harshbarger, 'Cloud Computing Providers and Data Security Law : Building Trust with United States Companies' (2011) 16 JTech L & Pol'y 229, 233.

the provision as required.[83]

5.2 Ease of Maintenance

CSP does not only offer users different kinds of services, ranging from software to infrastructure, but also provides maintenance of services. Cloud users can be sure at all times that the programmes are the latest version, without the need to reinstall or upgrade.[84]

5.3 Increase Effectiveness of IT Capabilities

The cloud computing capabilities are pooled together in a large resource and can be shared among users. They are instantly available for all users and their usage can be scaled up or down depending on the demands. Furthermore, cloud resources are not left idle during off-peak periods, as they can be used by other users.[85]

5.4 Increase the Flexibility

Compared with storage of information on a personal computer, storage in a cloud can be flexibly and automatically customised to users' needs. Cloud users can rapidly provision their own resources.

6. DRAWBACKS OF CLOUD COMPUTING: TECHNICAL ISSUES

6.1 Lack of Availability

Cloud computing enables users to gain access to services anywhere and at any time, as long as the Internet is available.[86] This means that constant connectivity should be maintained, unless access to the data in cloud computing cannot be achieved.[87] When the network is broken or disrupted, as in the case of a denial of service attack, cloud users are unable to gain access to data or take advantage of cloud services, even in cases of emergency. [88]

Moreover, the data stored in cloud computing would be at risk, in terms of being

[83] Sabharwal (n37) 2; Bauer and Adams (n38) 5.
[84] V. V. Arutyunov, 'Cloud Computing: Its History of Development, Modern State and Future Considerations' (2012) 39 STIP 176.
[85] Bauer and Adams (n38) 14.
[86] ibid (n38) 5.
[87] J. Dale Prince, 'Introduction to Cloud Computing ' (2011) 8 JERML 449, 456.
[88] ibid 455.

inaccessible at any time.[89] This is because the cloud capabilities are pooled to serve multiple users, resulting in the data of all users being stored in the same resource. If some of a user's data is attacked, then the whole resource may be seized by authorities, meaning that the data of other users held in the same resource could not be accessed.[90]

6.2 Lack of Adequate Performance

Generally, cloud services are provided to users with different levels of performance, depending on the package they purchase.[91] Although CSP could provide an on-demand service to their users, in some cases CSPs cannot offer an adequate level of performance to some users, as there might be some intensive transaction-oriented and data-intensive applications.[92] Additionally, there could be some problems causing service outages such that, in the case of denials of service, the CSP would be unable to guarantee provision of round-the-clock reliability to their users.[93] This situation would have an adverse effect on cloud users, such as in the case of business continuity.[94]

6.3 Lack of Portability

After cloud users have placed their data in cloud computing, they may decide to move their data out of a CSP if they are not satisfied with the service provided to them. However, the cloud infrastructure of several CSPs does not always employ the same approach for storing the data or applications of users.[95] Therefore, it might be difficult for cloud users to migrate their data or applications running on one CSP to other CSPs, since they may not interoperate with other provider's service.[96]

---

[89] Nick Perry, 'Popular File-Sharing Website Megaupload Shut Down' (*USA Today, 20 Jan 2012*) <http://usatoday30.usatoday.com/tech/news/story/2012-01-19/megaupload-feds-shutdown/52678528/1> accessed 1 March 2014.

[90] James Urquhart, 'FBI Seizures Highlight Law as Cloud Impediment' (*CNET, 22 April 2009*) <http://www.cnet.com/uk/news/fbi-seizures-highlight-law-as-cloud-impediment/> accessed 11 March 2014; Hon and Millard, 'Control, Security and Risks in the Cloud ' in Millard C (ed), *Cloud Computing Law* (Oxford University Press 2013,18.

[91] Arasaratnam (n4) 11.

[92] Furht (n38) 17.

[93] Jelena Mirkovic, Janice Martin and Peter Reiher, *A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms* (Computer Science Department, University of California, Los Angeles, Technical Report, 2004) 1; Furht (n38) 18.

[94] Arasaratnam (n4) 10.

[95] Voorsluys, Broberg and Buyya (n20) 35.

[96] Hon and Millard, 'Control, Security and Risks in the Cloud '(n90) 26.

6.4 Data Security Risks

The features of cloud computing are likely to bring risks to the security of data held in cloud computing, such as data being misused, lost, damaged or disclosed to third parties.[97] The features can be listed as follows: (a) cloud users do not have full physical control over their data[98] ;(b) cloud infrastructure is shared by a large number of users and one kind of service can be layered on another kind of service, so there may be more than one CSP involved in the same set of data processing[99]; (c) the data might be processed to, and stored in, many servers located anywhere around the world[100]; and (d) the data will usually be copied or replicated to different data centres without being deleted on removal to another data centre.[101]

7. LEGAL PROBLEMS

7.1 Data Protection Problems

7.1.1 Problems Regarding the Application of the EU Data Protection Law in Cloud Computing

The processing of personal data in cloud computing is subject to the EU DP law (which was the Data Protection Directive 95/46/EC (DPD) before being replaced by the General Data Protection Regulation (GDPR)).[102] However, there are three main legal problems arise when applying the DPD in the context of cloud computing, and these problems can still not be properly addressed by the GDPR. This is one of the key concerns of this thesis and will be thoroughly explored in Chapter 3. This section will only briefly explain these problems, as follows:

---

[97] See generally in Dan Svantesson and Roger Clarke, 'Privacy and Consumer Risks in Cloud Computing' (2010) 26 CLS Rev 391.
[98] Jansen and Grance (n52) 13.
[99] ICO, *Guideline on the Use of Cloud Computing* (9 May 2013), 6.
[100] Frank Alleweldt and others, *Cloud Computing* (European Parliament's Committee on Internal Market and Consumer Protection, 2012), 21.
[101] Samson Yosep Esayas, 'A Walk in to the Cloud and Cloudy it Remain: the Challenges and Prospects of 'Processing' and 'Transferring' Personal Data', 28 CLS REV 662, 664.
[102] The Data Protection Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of their Personal Data and on the Free Movement of such Data. And Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC. See more details in chapter 3, section 1.

7.1.1.1 Who is the Data Controller and the Data Processor when Personal Data is Processed in the Cloud?

Regarding the DPD, it might be assumed that the cloud user, who determines the purposes of, and means for, processing his/her personal data is the data controller (controller) and the CSP, who merely processes such data on behalf of the cloud user, is the data processor (processor).[103] Therefore, the cloud user bears most of burden to comply with the DP principles, while the CSP is required to act only on the instructions of the cloud user and to provide appropriate security measures in relation to the personal data processing.[104]

However, it is, in practice, quite difficult to determine the controller and the processor in the context of cloud computing. This is due to the ability to control the data processing in cloud computing being divided between the cloud user and the CSP, and who is actually the sole joint controller varies depending on the context. Therefore, it is uncertain whether the CSP is the controller or the processor, or neither, in different situations.[105] Hence, the situation in cloud computing does not fit the binary model set out by the DPD, as described above.

The GDPR attempts to addresses these problems by promoting the existing concept of joint controller and by placing greater obligations on processors, which perpetuates the binary assumptions in the DPD.[106] Therefore, the existing problems can still not be addressed by the GDPR, as the division in the control of the purposes of, and means for, data processing in cloud computing is no longer a binary division between the controller and the processor. Instead, it seems more like a sliding scale.

7.1.1.2 When Does the EU Data Protection Law Apply to the Processing of Personal Data Held in Cloud Computing and Which Member State Laws Apply to the Data Processing?

Regarding the DPD, CSPs will be subject to the EU DP law in circumstances where

[103] DPD, Art 2 (d)(e); A29WP, *Opinion 05/2012 on Cloud Computing* (01037/12/EN WP196, Adopted 1 July 2012) 7-8.
[104] DPD, Art 6, 17, 23.
[105] Paul Schwartz, 'Information Privacy in the Cloud' (2013)161 U. Pa. L. Re. 1623, 1626.
[106] GDPR, Art 26(1).

(i) CSPs were established in the EU (EU CSPs) and the processing was carried out in the context of the activities of such an establishment.[107]

(ii) CSPs were not established in the EU (non-EU CSPs), but such CSPs were using "equipment" in the EU to process personal data.[108]

Once CSPs fell under the scope of the DPD, they had to comply with the DP law of the Member State where

(i) the establishment of the EU CSPs was located and there was data processing taking place in the context of the activities of this establishment;[109]

(ii) the equipment used by non-EU CSPs for processing personal data was situated.[110]

However, it is not always easy to determine the territorial reach of the EU DP law and the applicable law in the context of cloud computing. In the case of EU CSPs, it is unclear what is meant by the terms "establishment" and "in the context of the activities of an establishment". The implications of courts' decisions are quite far-reaching and they lead to controversial issues with regard to their extraterritorial effects.[111] Multinational CSPs would thus have to comply with multiple and potentially conflicting national DP laws. In the case of non-EU CSPs, the "equipment" and "make use of equipment" grounds seem to have undesirable consequences for non-EU CSPs, who would be caught by the EU DP law.

The GDPR proposes a definition of the main establishment of the controller and the processor to deal with the problems regarding the territorial scope of the EU DP law when EU CSPs, who have more than one establishment, jointly determine the purposes of, and the means for, the data processing.[112] However, it could not fix such problems, as this concept is relevant to the applicable law, rather than to the territorial scope.

[107] DPD, Art 4(1)(a).
[108] DPD, Art 4(1)(c).
[109] DPD, Art 4(1)(a).
[110] DPD, Art 4(1)(c).
[111] Cedric Ryngaert, 'Editorial : Special Issue Extraterritoriality and EU Data Protection' [2015] IDPL 1, 1-5; Case C–131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González, CJEU, Judgment of 13 May 2014.
[112] GDPR, Art 4(16)(a) and (b).

Moreover, the GDPR introduces the "one stop shop" rule to address the situation when CSPs are subject to multiple and potentially conflicting rules of different national DP laws.[113] In this case, the applicable law would be the DP law of the jurisdiction of their leading Data Protection Authority (DPA).

In the case of non-EU CSPs, the GPDR introduces the connecting factors of "offering" and "monitoring", which seems to provide more certainty about the law that is applicable to the personal data processing in cloud computing.[114] Nevertheless, this tends to bring a lot more non-EU CSPs within the territorial scope of the EU DP law, as any CSP is presumably "offering" its service to the EU.

7.1.1.3 Can Personal Data Held in Cloud Computing be Transferred into Non-EU Cloud Computing?

The DPD set out data export rules to prohibit the transferring of personal data to non-EU countries (third countries), unless those countries can ensure an adequate level of DP.[115] However, the data residing in the cloud will usually be stored in, or processed to, various data centres located in different countries.[116] Furthermore, there might be more than one CSP involved in the same set of data processing, as in the case of sub-CSPs or sub-sub CSPs; thus, personal data held in cloud computing is likely to be transferred to different locations.[117] Accordingly, applying data export rules in the context of cloud computing often seems to be difficult.[118]

The GDPR improves the current situation by extending the scope of the data export rule to cover the "onward transfer" of personal data from a non-EU country to another non-EU country, in order that this would cover more scenarios of data transfer

[113] GDPR, Art 56.
[114] GDPR, Art 3(2)(a) and (b).
[115] DPD, Art 25.
[116] Alleweldt and others (n100) 82.
[117] A29WP, *Opinion 05/2012 on Cloud Computing* (n 103) 17; J. Nancy King and V.T. Raja, 'What Do They Really Know About Me in the Cloud? A Comparative Law Perspective on Protecting Privacy and Security of Sensitive Consumer Data' (2013) 50 Am Bus LJ 413, 435.
[118] W Kuan Hon and Christopher Millard, 'How Do Restrictions on International Data Transfers Work in Clouds? ' in Christopher Millard (ed), *Cloud Computing Law* (OUP 2013) 254; Kenneth N. Rashbaum, Bennett B. Borden and Theresa H. Beaumont, 'Outrun the Lions: A Practical Framework for Analysis of Legal Issues in the Evolution of Cloud Computing' (2014) 12 Ave Maria L REV 71, 80-82.

within cloud computing.[119] However, this would create difficulties for EU data subjects to enforce their rights against such non-EU data importers and exporters.

As well as that, there are problems that prevent the lawful basis for transferring data outside the EU set out by the DPD from working effectively to provide an adequate level of protection to the data held in cloud computing. For example, the unclear meaning of "unambiguous" consent of the data subjects makes it difficult to identify the meaningful consent that achieves compliance with the data export rule under the DPD.[120] The Standard Contractual Clauses (SCCs)) were limited and inflexible regarding the actors and their circumstances of involvement.[121] Although Binding Corporate Rules (BCRs) were not explicitly recognised in the DPD, the Member State DPA did recognise them as the legal basis for international data transfer under Article 26(2) of the DPD. However, BCRs are limited only to the data transfer within the same corporate group and the implementing BCRs are, in practice, quite cumbersome, expensive and time-consuming.[122] The EU-US Safe Harbor Agreement was ruled to be invalid by the CJEU in 2015 because it did not provide an adequate level of protection of the data transferred from the EU to the US.[123]

The GDPR deals with the existing situations by introducing more types of SCCs to cover more scenarios of data transfer in cloud computing.[124] The GDPR, for the first time, formally recognises BCRs and extends its scope to cover the data transfer between 'a group of undertakings, or a group of enterprises engaged in a joint economic activity, including their employee'.[125] However, it remains unclear whether or not sub-CSPs will be part of such a group of enterprises engaged in a joint economic activity.

Although the GDPR replaces "unambiguous" consent of the data subjects in the DPD by "explicit" consent, it remains difficult to obtain valid consent from the data

[119] GDPR, Rec 101 and Art 44.
[120] DPD, Article 26(1)(a).
[121] DPD, Article 26(2).
[122] See a list of A29WP working papers on BCRs, at < http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/tools/index_en.htm > accessed 1 April 2018.
[123] Case C-362/14 Maximillian Schrems v Data Protection Commissioner [2015] CJEU No. 117/15, judgment of 6 October 2015.
[124] GDPR, Article 46(2)(c)(d) and Article 46(3)(a).
[125] GDPR, Article 47.

subjects in cloud computing, resulting in greatly limiting its availability for cloud computing.[126] The GDPR does nothing to address the criticisms of the EU-US Safe Harbor Agreement. The EU-US Privacy Shield was adopted to replace the EU-US Safe Harbor Agreement in aiming to ensure an adequate level of DP under Article 45 of the GDPR, but its validity is currently facing a number of legal challenges.[127]

7.1.2 Problems Emerging from the EU and US Legal Frameworks Governing Access to Personal Data held in Cloud Computing by Law Enforcement Agencies (LEAs) and Nation Intelligence Agencies (NIAs)

Due to the fact that there are various kinds of data residing in cloud computing, ranging from general to confidential data, LEAs and NIAs will seek to obtain access to data in cloud computing, that relates to potential criminal activity, located in different countries for preventing, investigating, detecting and prosecuting crimes and acts of terrorism. CSPs may be obliged by law to allow such agencies to obtain access to their users' data or, in some cases, such agencies might spy on the data without acknowledgement of this by CSPs.[128] These situations would inevitably pose a serious threat to the privacy of cloud users. This is another key concern of this thesis and will be further explored in Chapter 4.

This thesis focuses only on the problems regarding the access to personal data of EU cloud users entrusted with US based CSPs by US LEAs and NIAs. These problems were brought to the public's attention by the PRISM scandal, in which it was revealed in 2013 by Edward Snowden, a former employee of CIA and US National Security Agency(NSA), that US agencies had spied on the data of EU citizens held by the nine leading US internet companies, e.g. Google, Yahoo and Facebook, under the surveillance programme called PRISM.[129] It was also alleged that the UK Intelligence

[126] GDPR, Article 49(1)(a).
[127] European Parliament, *Commission Implementing Decision of 12.7.2016 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield* (Brussels, 1272016 C(2016) 4176 final).
[128] Wolf C and Cohen B, *Pan-American Governmental Access to Data in the Cloud* (A Hogan Lovells White Paper, 17 July 2014).
[129] Barton Gellman and Laura Poitras, "U.S., British intelligence mining data from nine U.S. Internet companies in a broad secret program", Washington Post, 6 June 2013. <http://articles.washingtonpost.com/2013-06-06/news/39784046_1_prism-nsa-u-s-servers > accessed 12

Agency, named the Government Communication Headquarters (GCHQ), tapped into global telecom cables for mass monitoring of the personal data of EU citizens, for example, email messages, Facebook posts and telephone calls, under a surveillance operation codenamed TEMPORA, and that it, too, gathered personal data through the US PRISM programme.[130]

The main cause of these problems is the traditional and formal legal approaches that allow the US LEAs to acquire the personal data of EU data subjects for law enforcement purposes do not work satisfactorily enough to protect the privacy of the EU data subjects.[131] And this situation tends to provide an opportunity for intelligence agencies to circumvent their domestic oversight regimes by asking their foreign partners to undertake intelligence activity they cannot perform legally.[132]

Apart from that, the US and the EU have different expectations of legal protection and legal regimes around privacy protection. The US legal frameworks that cause considerable anxiety regarding the privacy of EU data subjects are the Foreign Intelligence Surveillance Act of 1978 (FISA)1978, the USA Patriot Act 2001 and the Foreign Intelligence Surveillance Amendments Act of 2008 (FISAA) 2008, which contain provisions that allow for discrimination between US and non- US persons.[133] The requirements imposed by such legal frameworks for carrying out electronic surveillance on US persons seem to be higher than those for non-US persons.[134] Accordingly, the data of EU cloud users stored in a US data centre may neither be

---

September 2013.

[130] Ewen MacAskill and others, 'GCHQ Taps Fibre-Optic Cables for Secret Access to World's Communications' (*The Guardian*, 21 June 2013) <http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa> accessed 12 September 2014.

[131] See section 7.4.

[132] Ian Brown and Douwe Korff, 'Foreign Surveillance: Law and Practice in a Global Digital Environment' 3 EHRLR 243, 243.

[133] ibid.

[134] For example, while the electronic surveillance conducted on non-US persons can be approved for the period of up to one year, but such surveillance conducted on US persons can only be approved for no more than 90 days. See 50 U.S.C. § 1805(d)(1).

protected at the same level as their own government provides, nor be protected at the same level as the US government provides to its own citizens.[135]

Following the Snowden revelations, the EU and the US introduced many legal instruments to increase the level of privacy protection to EU data subjects, such as the Judicial Redress Act of 2015 and the EU-US Privacy Shield and the Cloud Act 2018, with a view to increasing trust between the EU and the US. However, the existing problems do not yet seem to be properly addressed. This has caused major concern for EU cloud users, in that the activities of public agencies obtaining access to their personal data entrusted with the US CSPs may violate the privacy rights of EU data subjects, and, in some cases, such access is even authorised by US laws. This situation would potentially create risks regarding the privacy of EU cloud users, which would then inevitably affect the level of user trust in cloud computing, at least to some extent. These problems urgently need to be addressed with a view to balancing national security and individuals' privacy. As Reding stated in the EU-U.S. Ministerial meeting held on 14 June 2013 when she was the Vice-President of the Commission for Justice, 'the concept of national security does not mean that anything goes: States do not enjoy an unlimited right of secret surveillance'.[136]

7.2 Contractual Problems

Normally, the relationship between CSPs and cloud users is bound by a standard terms contract.[137] Although this contract is often offered on a "take it or leave it" or adhesion basis, it can sometimes be negotiated.[138] This contract may be known as Terms of Service (TOS), Service Level Agreement (SLA), Acceptable Use Policy (AUP) or

[135] See generally in Swire P and Kennedy-Mayo D, 'How Both the EU and the US Are "Stricter" Than Eact Other for the Privacy of Government Requests for Information ' (2017) 66 Emory LJ 617.
[136] Viviane Reding, *PRISM Scandal: Vice-President Reding Makes it Clear the Data Protection Rights of EU Citizens are Non-Negotiable* (EU-US Ministerial held on 14 June 2013).
[137] Carlos A. Rohrmann and Juliana Falci Sousa Rocha Cunha, 'Some Legal Aspects of Cloud Computing Contracts' (2015) 10 JICLT 37, 41.
[138] Timothy J. Calloway, 'Cloud Computing, Clickwrap Agreements, and Limitation on Liability Clauses : A Perfect Storm?' (2012) 11 Duke L & Tech Rev 163;W Kuan Hon, Christopher Millard and Ian Walden, 'Negotiated Contracts for Cloud Services' in Christopher Millard (ed), *Cloud Computing Law* (Oxford University Press 2013).

Privacy Policy.[139]

It has been found in many research projects that cloud contracts are normally written in a way that favours CSPs over cloud users in some aspects.[140] Some specifically exclude liability for any damage to users' data.[141] Some preserve a right to terminate users' access to their services at any time, without giving any notice, for any reason whatsoever.[142] Although such contractual clauses seem to be inappropriate, unfair and unenforceable, the Unfair Contract Terms Directive (UCTD) does not explicitly indicate whether or not cloud users are bound by these terms.[143] Therefore, the national law would be the main instrument for determining the legal effects of all such contract terms. However, after the Commission had examined the national rules on contract law and those that apply to cloud computing, there are only a few legal systems, such as in Germany and Latvia, that impose specific consequences on those contract terms.[144]

Accordingly, issues regarding unclear and unfair terms of cloud contracts have been receiving much attention from the Commission as problems that need to be addressed urgently.[145] An Expert Group on Cloud Computing Contracts composed of various entities, such as CSPs, users and representatives of legal professions who have expertise in cloud contracts, was set up by the Commission to define safe and fair conditions and identify the best practices for cloud contracts.[146] The Commission also launched a comparative legal study on cloud contracts to supplement the work of this

[139] Terms of Service (TOS) contains the overall detail of relationship between CSP and users , such as commercial terms or choice of law; Service Level Agreement (SLA) contains the level of service provided by the cloud provider; Acceptable Use Policy (AUP) contains the rule for using service, and Privacy Policy contains the provider's approach for holding, managing the customers' data.

[140] Simon Bradshaw, Christopher Millard and Ian Walden, 'Standard Contracts for Cloud Service' in Christopher Millard (ed), *Cloud Computing Law* (Oxford University Press 2013); Stylianou K, Venturini J and Zingales N, 'Protecting User Privacy in the Cloud: An Analysis of Terms of Service' (2015) 6 EJLT 1.

[141] Amazon Web Service Customer Agreement, section 11: limitations of liability <http://aws.amazon.com/agreement/> accessed 19 March 2018.

[142] Rackspace Website Term of Use, section Content you Submit <Http://www.rackspace.co.uk/legal/website-terms-of-use> accessed 19 March 2018.

[143] European Commission's Expert Group on Cloud Computing Contracts, *Unfair Contract Terms in Cloud Computing Service Contracts* (Discussion Paper, 5-6 March 2014) 2.

[144] Commission, *Unleashing the Potential of Cloud Computing in Europe* (Brussels, 2792012 COM(2012) 529 final) 11.

[145] ibid 10.

[146] Commission Decision of 18 June 2013 on Setting up the Commission Expert Group on Cloud Computing Contracts.

expert group.[147]

7.3 Intellectual Property Problems

Cloud computing is being increasingly used to store Intellectual Property (IP) assets, as they provide a clear and easy-to-follow chain of custody and reduce the unstructured human interactions with the data.[148] However, cloud computing may also increase the opportunities for copyright infringement, since it can offer a convenient way to gain access to IP contents anywhere and at any time via any type of device over the Internet without the permission of the IP right holders, and this access may lead to illegal content.[149]

In fact, there are two approaches that are often implemented with a view to preventing IP infringement in cloud computing.[150] Firstly, technological means, for example, Digital Right Managements (DRMs), are used to prevent other people from copying the copyright materials supplied to cloud computing. Secondly, cloud contractual terms are used between CSPs and cloud users, for example by requiring cloud users not to store anything if they do not have the permission of the right holder.[151] However, the activities of cloud users cannot always be adequately controlled by CSPs, as can be seen in the case of Megaupload, a well-known file sharing and storage website, which was shut down after being indicted by the US Federal Court Grand Jury for criminal copyright infringement and conspiracy of money laundering in 2012.[152]

Furthermore, cloud computing could entail IP issues in relation to who owns the

---

[147] Commission, *Comparative Study on Cloud Computing Contracts* (Prepared by DLA Piper UK LLP March 2015); Commission, *European Cloud Initiative - Building a Competitive Data and Knowledge Economy in Europe* (Brussels, 1942016 COM(2016) 178 final).

[148] Heidi Salow, 'Keeping your Intellectual Property in the Cloud' Intellectual Asset Management March/April 2014 <https://thomsonipmanagement.com/docs/downloads/iam_cloud_software_hsalow_0214.pdf> accessed 1 November 2014.

[149] George Jiang, 'Rain or Shine : Fair and Other Non-Infringing Uses in the Context of Cloud Computing' (2010) 36 Journal of Legislation 395, 395: Weber RH and Nicolaj Staige D, 'Cloud Computing: A Cluster of Complex Liability Issues' (2014) 20 Web JCLI.

[150] Chris Reed and Alan Cunningham, 'Ownership of Information in Clouds' in Christopher Millard (ed), *Cloud Computing Law* (Oxford University Press 2013) 152.

[151] ibid.

[152] US v Kim Dotkom, 12-00003, US District Court, ED Virginia, Document 107, 21 June 2012.

materials produced in cloud computing.[153] Normally, the IP rights over the materials held in cloud computing are determined by the clauses of a cloud contract.[154] However, in the absence of such clauses, the Intellectual Property law, for example the Copyright law and the Database Directive, would come into play. The location of where the materials are produced is very important, due to the different jurisdictions perhaps having different rules for determining the ownership of such materials.[155]

Having said that, identifying who own the materials produced in cloud computing is quite a difficult task, as the materials residing in the cloud may have been processed to, and stored in, several servers located anywhere around the world; hence, the location of where the materials were produced is not easy to determine.[156] Even identifying the exact actors who produce the materials held in cloud computing may prove to be difficult, as there could be many actors involved in the same data processing for delivering cloud services.[157]

7.4 Crime and Forensic Problems

Cloud computing is perceived as a very convenient target, a kind of "one-stop shopping" for criminals, due to various kinds of user data residing in cloud computing.[158] The existing legal frameworks for fighting cybercrime in cloud computing do not seem to be working effectively. The Convention on Cybercrime, which set out the rules for international cooperation between countries in investigating and prosecuting cybercriminals, has been considered to be largely a symbolic policy, having only a

---

[153] Svantesson D and Clarke R, 'Privacy and Consumer Risks in Cloud Computing' (2010) 26 CLS Rev 391, 391.

[154] Facebook, Statement of Rights and Responsibilities section 2. Sharing Your Content and Information < https://www.facebook.com/legal/terms/update > accessed 11 January 2018.

[155] For example, the US has no database rights like the EU. Therefore, the database which consists of factual information will not be subsisted by any IP rights in the US. However, if such database involves some creative expression, it can be protected by copyright as a compilation. On the other hand, if the database is recorded by an English company on a server in EU Member State, this database will receive protection by the Database Directive.

[156] Alleweldt and others (n100) 21.

[157] Chris Reed and Alan Cunningham, 'Ownership of Information in Clouds' in Christopher Millard (n150) 144.

[158] See generally in Alice Hutchings, Russell G. Smith and Lachlan James, 'Criminals in the Cloud: Crime, Security Threats, and Prevention Measures' in Russell G. Smith, Ray Chak- Chung Cheung and Laurie Yiu- Chung Lau (eds), *Cybercrime Risks and Responses* (Springer 2015).

limited effect on combating cyber crime.[159] Mutual Legal Assistance Treaties between the US and the EU have, in practice, faced various problems, such as being costly, slow and cumbersome.[160]

Additionally, cloud computing can impede cybercrime investigations and digital forensics, as it is quite difficult to identify the sources of potential evidence in cloud computing, due to the fact that the data can be processed and located across numerous servers.[161] Although there are forensic tools for preserving evidence on remote computer systems, difficulties still exist in acquiring data remotely from cloud servers in a forensically sound manner.[162] For instance, if evidence comprising of child pornography is uploaded to cloud storage, taking snapshots or videoing may not be sufficient evidence. This is because the evidence merely confirms the existence of the data, rather than determining whether the data really belonged to the suspect and confirming that the suspect is the one who actually uploaded the data to cloud computing. The investigators may, thus, face challenges regarding the reliability of the data.[163]

CONCLUSIONS

Cloud computing is a model for providing computing resources over the Internet, ranging from simply providing an outsourced storage space to the full external provision of hardware infrastructure. While many users enjoy using various types of cloud service, some remain hesitant to take advantages offered by cloud computing, due to the technical and legal problems related to cloud computing that pose risks and a great deal

[159] Nancy E. Marion, 'The Council of Europe's Cyber Crime Treaty: An exercise in Symbolic Legislation' (2010) 4 IJCC 699, 702.
[160] Cristos Velasco, Julia Hörnle and Anna-Maria Osula, 'Global Views on Internet Jurisdiction and Trans-border Access : Current Developments in ICT and Privacy/Data Protection' in Serge Gutwirth, Ronald Leenes and Paul De Hert (eds), *Data Protection on the Move* (Law, Governance and Technology Series 24, Springer 2016) 469.
[161] Mark Taylor and others, 'Forensic Investigation of Cloud Computing Systems' 2011 Network Security 10, 6; Stavros Simou and others, 'A Survey on Cloud Forensics Challenges and Solutions' (2016) 9 Security and Communication Networks 6285, 6286.
[162] Aqil Burney, Muhammad Asif and Zain Abbas, 'Forensics Issues in Cloud Computing' (2016) 4 JCC 63, 67.
[163] See generally Stavros Simou and others, 'Cloud Forensics: Identifying the Major Issues and Challenges' in Alice Hutchings, Russell G Smith and Lachlan James (eds), *Advanced Information Systems Engineering 26th International Conference, CAiSE 2014 Thessaloniki, Greece, June 16–20, 2014 Proceedings* (Springer).

of uncertainty for cloud users in various aspects.[164] As the legal problems around DP do affect the privacy of cloud users, and this is considered to be the key concern among cloud users, these problems are very likely to weaken user trust in cloud computing. And this aspect, focusing on how user trust in cloud computing is affected, will be explored in the subsequent chapters, in order to determine possible approaches that may enhance user trust in cloud computing, with a view to increasing the use of cloud computing.

However, this thesis will focus only on the two legal problems relating to DP: (1) problems regarding the application of the EU DP law to the processing of personal data in cloud computing; and (2) problems regarding the EU and the US legal frameworks governing access to personal data held in cloud computing by LEAs and NIAs. Before discussing these two problems in Chapters 3 and 4, the next chapter will explore the issue of trust in cloud computing, to gain an understanding of what creates trust, what breaks trust and how to build trust.

[164] See empirical evidence in chapter 2, section 2.2.

CHAPTER 2

THE CONCEPT OF TRUST IN CLOUD COMPUTING

INTRODUCTION

During the past few years, especially after the revelation in 2013 of the mass surveillance programme (called "PRISM") conducted by the United States (US) National Security Agency (NSA), cloud users have been becoming aware of the privacy risks presented by cloud computing. Many surveys have revealed that European Union (EU) cloud users are feeling reluctant about adopting cloud services, due to their trust being affected by these risks.[1] Accordingly, trust does seem to play a crucial role in the cloud system, as it can either facilitate or prevent individuals and SMEs from adopting cloud computing. Therefore, as cloud computing could be a main driver of economic development, the problems relating to lack of trust in cloud computing have been receiving a great amount of attention from the public and this has become a pressing issue that needs to be addressed.

The objective of this chapter is to address Research Question C: What does trust mean in the context of cloud computing and why is it important? This involves four sub-research questions, as follows:

(1) How is trust perceived by different disciplines?

(2) What are the key definitions of trust in cloud computing?

(3) Do individuals and SMEs trust cloud computing?

(4) What are the criteria for creating trust in cloud computing?

There are two main sections in this chapter. After this introduction will be a description of trust from different disciplines, namely psychology, sociology, business and electronic commerce, followed by an analysis of the characteristics of trust from the author's own viewpoint, in section one.

Section two will explore the concept of trust in cloud computing in relation to

[1] See more details in section 2.2.

three main points, as follows:

(1) key definitions of trust in cloud computing;

(2) an analysis of whether individuals and Small and Medium Sized Enterprises (SMEs) trust cloud computing, based on empirical evidence from various sources; and

(3) the criteria for creating trust in cloud computing.

Finally, conclusions will be drawn from discussion of various points raised in this chapter.

1. TRUST FROM DIFFERENT DISCIPLINES

Trust is one type of belief that comes into play in any attempt to rationalise people's decisions in a situation where there is an ***incomplete evidence***.[2] Trust has been perceived as an integral part of our daily life. Without trust, most of our everyday human cooperation might not be possible.[3] However, despite trust being perceived as a concept familiar to everyone, it is still challenging to define the exact meaning of trust, as it can be explored from different disciplines. Consequently, there remains no universally agreed definition of trust.

Before exploring the concept of trust in cloud computing, it is worth considering a multidisciplinary view of trust by focusing on: (1) how trust can be created, and under what circumstances; (2) what breaks trust; and (3) how trust can be rebuilt.

1.1 Psychology

Psychologists have commonly focused on the interpersonal relationships between individuals. Therefore, trust is seen as a state of expectation on the part of a trustor towards a trustee under circumstances of uncertainty.[4] Gambetta viewed that trust could be viewed as a mental mechanism that helps reduce uncertainty in order to promote

[2] Arion WJ, Burchell B and Burchell A, 'Specific Inactivation of the Phospohydrolase Component of the Hepatic-Microsomal Glucose-6-Phosphatase System by Diethyl Pyrocarbonate' (1984) 220 Biochem J 835 as cited in Florian Egger, 'Consumer Trust in E-Commerce; From Psychology to Interaction Design' in J.E.J. Prins and others (eds), *Trust in Electronic Commerce : The Role of Trust from a Legal an Organisational and a Technical Point of View* (Kluwer Law International 2002), 17.

[3] Niklas Luhmann, 'Familiarity, Confidence, Trust: Problems and Alternatives' in Diego Gambetta (ed), *Trust: Making and Breaking Co-operative Relations* (Wiley-Basil Blackwell 1988) 97.

[4] Diego Gambetta, 'Foreward' in Diego Gambetta (ed), *Trust: Making and Breaking Cooperative Relations* (Oxford: Basil Blackwell 1988).

relationships.[5] The most often cited definition of trust, provided by Rousseau et al., is that 'trust is a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another'.[6]

From a psychological viewpoint, trust is based on an individual theory that can be applied to various contexts in different relationships. Consequently, there are probably many factors that can generate the relationship between trusting and being trustworthy. Hawthorn stated that trust may be unable to generate itself and, therefore, it requires something analogous to impose the initial conditions of its generation.[7] What creates trust is some combination of (1) ***an availability of information***, which is necessary for building relationships, such as information about the reputation, ability and past behaviour of the trustees; (2) ***great potential for successful communication,*** which will help reduce the ambiguity of the situation; (3) ***mutual understanding,*** which will lead to great cooperation; (4) ***no potential for unexpected threat***; and (5) ***risks that can be evaluated***, but the perception and the evaluation of risk are highly subjective.[8]

Molleting suggested that it takes a long time for trust to be developed, since it needs an ongoing process to build on reasons and routines.[9] Prof. Hirschman viewed that 'trust, like other moral resources, grows with use and decays with disuse'.[10] Once trust is broken, the deeply distrustful attitude is very difficult to invalidate through the above factors and this prevents people from engaging in any relationships.[11]

1.2 Sociology

Trust is examined in the context of social relationships as an orientation towards society

---

[5] Diego Gambetta, 'Can We Trust Trust?' in Diego Gambetta (ed), *Trust: Making and Breaking Cooperatives* (Basil Blackwell 1988) 217-8.
[6] Denise M Rousseau and others, 'Not so Different After All : a Cross-Discipline View of Trust' (1998) 23 AMR 393, 395.
[7] Gedffrey Hawthorn, 'Three Ironies in Trust' in Diego Gambetta (ed), *Trust: Making and Breaking Coorperative Relations* (Basil Blackwell 1988), 125.
[8] David Good, 'Individuals, Interpersonal Relations, and Trust' in Diego Gambetta (ed), *Trust: Making and Breaking Cooperative Relations* (Basil Blackwell 1988) 33, 36-38 and 45; Luhmann (n3) 100.
[9] Guido Mollering, *Trust: Reason, Routine, Reflexivity* (Elsevier 2006) 111.
[10] Albert O Hirschman, 'Against Parimony : Three Easy Ways of Complicating Some Categories of Economic Discourse' (1984) 74 Am Econ Rev 88, 93.
[11] Gambetta, 'Can We Trust Trust?' (n5) 234.

and towards others that have social meaning.[12] The situation of trust is described by Gambetta as 'a subclass of those involving risk…. They are situations in which the risk one takes depends on the performance of another actor'.[13]

As with the psychological view, social trust is seen as a dynamic process that must be built up over time.[14] It is based on cultural values and moral norms that vary across people, contexts and time.[15] Social trust in Earle and Cvetkovich's view is a relational process that requires evidence of the competence, responsibility and prior action of individuals or institutions.[16] This would enable trustors not to consider other alternative possibilities in order to avoid risks/disappointment, but they would have to neglect, more or less, the possibility of such disappointment for the sake of associated advantages.[17]

Social trust is closely linked with reputation, which is usually acquired gradually through past behaviour over time in well-understood circumstances, or sometimes by pure chance, but which can also be destroyed by misfortune or by pursuing certain courses of action.[18] In the study by Bradbury et al., trust is closely linked to honesty, openness and accountability.[19] Slovic claimed that social trust is fragile and is typically generated slowly, but could be destroyed very quickly.[20] Luhmann, a famous professor of sociology, opined that lack of trust could lead to people withdrawing from activities and, as a result, a system may lose size, as it may shrink below the critical threshold

---

[12] Tom R. Tyler and Roderick M. Kramer, 'Whither Trust' in Tom R. Tyler and Roderick M. Kramer (eds), *Trust in Organisations: Frontiers of Theory and Research* (Sage Publications 1996) 5.
[13] James S. Coleman, *Foundations of Social Theory* (Harvard University Press 1994) 91.
[14] David G. Carnevale, *Trustworthy Government : Leadership and Management Strategies for Building Trust and High Performance* (San Francisco : Jossey-Bass 1995) 199; see generally in Adam B. Seligman, 'Trust and Sociability: On the Limits of Confidence and Role Expectations' (1988) 57 AJES 391; Vincent Buskens, 'The Social Structure of Trust' (1988) 20 Soc Networks 265.
[15] Uslaner EM, *The Moral Foundations of Trust* (CUP 2002) 2.
[16] Timothy C. Earle and George Cvetkovich, 'Social Trust and Culture in Risk Management' in George Cvetkovich and E. Ragnar Lofstedt (eds), *Social Trust and the Management of Risks* (Earthscan Publications 1999) 9-10.
[17] Luhmann (n3) 97.
[18] Partha Dasgupta, 'Trust as a Commodity ' in Diego Gambetta (ed), *Trust: Making and Breaking Cooperative Relations* (Basis Blackwell 2012) 59, 62.
[19] Judith A. Bradbury, Kristi M. Branch and Will Focht, 'Trust and Public Participation in Risk Policy Issues' in George Cvetkovich and Ragnar E. Lofstedt (eds), *Social Trust and the Management of Risk* (Earthscan Publications Ltd 1999) 119.
[20] Paul Slovic, 'Perceived Risk, Trust and Democracy' in George Cvetkovich and Ragnar E. Lofstedt (eds), *Social Trust and the Management of Risk* (Routledge 1999) 45-6.

necessary for its own reproduction at a certain level of development.[21]

1.3 Business

Trust is perceived in terms of utility or calculative processes as an expectation about another person, based on calculations that weigh the costs and benefits of a particular action to either the trustor or the trustee.[22] Bradach and Eccles defined trust as 'a type of expectation that alleviates the fear of one's exchange partner acting opportunistically'.[23] Powell stated that trust could be the critical lubricant in an economic exchange, in that it reduces the complex realities more effectively than prediction or bargaining.[24]

Moreover, trust can help maximise the utility and decrease the cost of transactions between parties, thus fostering business activities, employment and prosperity.[25] Many studies link trust to economic development as a precondition for superior performance and competitive success in the business environment.[26] Fukuyama even claimed that economic success depends on the level of trust that is inherent in the society.[27] This is because trust can lower the perceived risks and make production and exchange possible between partners.[28] DeGeorge demonstrated that, if the minimum level of trust was absent, business transactions would prove impossible, and then that would lead to the

[21] Gambetta, 'Can We Trust Trust?'(n5) 104.
[22] Christel Lane, 'Introduction: Theories and Issues in the Study of Trust' in Christel Lane and Bachmann. Reinhard (eds), *Trust Within and Between Organisations : Conceptual Issues and Empirical Applications* (Oxford University Press 2000) 5.
[23] Jeffrey L. Bradach and Robert G. Eccles, 'Price, Authority and Trust : From Ideal Types to Plural Forms' (1989) 15 Annu Rev Sociol 97, 104.
[24] Walter W. Powell, 'Neither Market Nor Hierarchy: Network Forms of Organization' (1990) 12 Res Organ Behav 295, 323.
[25] Robert M. Morgan and Shelby D. Hunt, 'The Commitment-Trust Theory of Relationship Marketing' (1994) 58 JM 20, 20.
[26] See generally in Sjoerd Beugelsdijk, Henri L.F. de Groot and Anton B.T.M. van Schaik, 'Trust and Economic Growth: A Robustness Analysis' (2004) 56 Exford Economic Paper 118; Paul J. Zack and Stephen Knach, 'Trust and Growth' (2001) 111 EJ 295; Patrick Francois and Jan Zabojnik, 'Trust, Social, Capital, and Economic Development' (2005) 3 JEEA 51; Mari Sako, 'Does Trust Improve Business Performance?' in Christel Lane and Reinhard Bachmann (eds), *Trust Within and Between Organisations: Concept Issues and Empirical Applications* (Oxford University Press 2000).
[27] Francis Fukuyama, *Trust: The Social Virtues and the Creation of Prosperity* (Free Press, New York 1995) 7.
[28] Dasgupta (n18) 64; see generally in George A. Akerlof, 'The Market for "Lemons": Quality Uncertainty and the Market Mechanism' (1970) 84 Q J Econ 488.

failure of the market.[29] The level of trust needed has an inverse relationship to the degree of risk with regard to each transaction.[30]

1.4 Electronic Commerce

Trust has long been identified as a very important factor in facilitating online trade transactions, which are more anonymous, impersonal and automated, compared with the traditional trade transactions in the physical world. [31] Nissenbaum indicated that 'without sufficient trust in online services, people will be reluctant to make use of such resources in part, due to the increased exposure to harm'.[32]

Before exploring the ways in which trust could be built in electronic commerce, it should be taken into account that both the system reliability and the trustworthiness of sellers can affect user trust in electronic commerce; hence, two main types of trust come into play.[33] First is trust in technology, which is the subjective probability by which an organisation assesses whether the underlying technological infrastructure and control mechanisms are capable of facilitating transactions according to their expectations.[34] The perceived trustworthiness of technology is based on three related factors:

(1) *functionality* - whether the technology delivers on the functionality promised by providing the feature sets needed to complete the task;

(2) *helpfulness* - whether the technology's help function provides the advice necessary to complete a task;

---

[29] Richard T. DeGeorge, *Competing with Integrity in International Business* (NewYork: Oxford University Press 1993) 21.

[30] See generally in Dean Povey, *Developing Electronic Trust Policies Using a Risk Management Model* (Proceedings of 1999 CQRE (Secure) Congress, Germany, 1999).

[31] Pauline Ratnasingam, 'Trust in Inter-Organizational Exchanges: a Case Study in Business to Business Electronic Commerce' (2005) 39 Decis Support Syst 525, 525-526; see generally in
Kiku Jones and Lori N.K. Leonard, 'Trust in Consumer-to-Consumer Electronic Commerce' (2008) 45 Inform Manage 88;Parvin Abbasi, Bahram Sadeghi Bigham and Saeed Sarencheh, 'Good's History and Trust in Electronic Commerce' (2011) 3 Procedia Comput Sci 827, 827-828.

[32] Helen Nissenbaum, 'Securing Trust Online : Wisdom or Oxymoron?' (2001) 81 BUL Rev 101, 106.

[33] Sonja Grabner Kraeuter, 'The Role of Consumers' Trust in Online-Shopping' (2002) 39 J Bus Ethics 43, 47.

[34] Pauline Ratnasingam and Paul Pavlou, 'Technology Trust in Internet-based Interorganizational Electronic Commerce' in Mehdi Khosrow-Pour (ed), *The Social and Cognitive Impacts of E-Commerce on Modern Organizations* (Idea Group Publishing 2004) 312.

(3) *reliability* - whether the technology works consistently and predictably.[35]

Second is trust in the trading partner, which relates to the vulnerability of one partner with regard to the other, which relies on previous experience of social and economic exchanges between the partners. The personal information of partners, for example the size, the brand and the reputation of partners, is also a critical factor that can either have a positive or a negative impact on users' trust.[36]

Prins et al. drew the conclusion that three major approaches can be used to build trust in electronic commerce.[37] Firstly, trust can be achieved by using technology. Various technical measures are employed for preserving information security, such as cryptography and pseudonymisation.[38] The design of websites, including content, structure, navigation and graphics, can also help in communicating the reliability of the site and promoting the brand and reputation of each online vendor.[39] A user-friendly web interface can increase the familiarity of users with an online vendor and its electronic commerce procedures and that can help in encouraging users' willingness to purchase and return.[40]

Secondly, trust can be established by using an agreement. Normally, buyers and

---

[35] D Harrison McKnight and others, 'Trust in Specific Technology: An Investigation of Its Components and Measures' (2011) 2 ACM TMIS 12, 12:5-12:9; D. Harrison McKnight, 'Trust in Information Technology' in B. Gordon Davis (ed), *The Blackwell Encyclopedia of Management Information System*, vol 7 (Wiley-Blackwell 2005), 329-331.

[36] Egger (n2) 5.

[37] Corien Prins and Leo Van Der Wees, 'E-Commerce and Trust : a Variety in Challenges' in J.E.J. Prins and others (eds), *Trust in Electronic Commerce : The Role of Trust from a Legal an Organisational and a Technical Point of View* (Kluwer Law International 2002) 5.

[38] Cryptography is a technical measure based on mathematical techniques. The data will be applied by means of an algorithm for transforming the data into another language which cannot be understood by other people. There are two types of cryptography:(1) one-way cryptography (hashed) – which is irreversible (2) two-way cryptography (encrypted) – which is reversible; See Keith M. Martin, *Everyday Cryptography: Fundamental Principles and Applications* (Oxford University Press 2012); Ross Anderson, *Security Engineering - A Guide to Building Dependable Distributed Systems* (2rd ed, John Wiley & Sons 2008) Chapter 5.
Pseudonymisation is a technical measure for disguising identity. This measure enables the collection of additional data in relation to the same individual without knowing his identity. Pseudonymisation can be done in both a retraceable and a non-retraceable way using different techniques; See A29WP, *Opinion 4/2007 on The Concept of Personal Data* (01248/07/EN WP 136, Adopted 20 June 2007, 2007), 18.

[39] Sabine Einwiller, *The Significance of Reputation and Brand for Creating Trust in the Different Stages of a Relationship between an Online Vendor and its Customers* (Eighth Research Symposium on Emerging Electronic Markets, 2001) 2.

[40] Juergen Noll, 'European Community & E-Commerce: Fostering Consumer Confidence' (2002) 9 EDI L Rev 207, 209-210.

sellers are bound by an online agreement. Most online buying sites have attempted to attract consumers through their quality and legally enforceable contractual clauses, such as privacy policy, warrantees and redress mechanisms (Alternative Dispute Resolution (ADR), Online Dispute Resolution(ODR)).[41] For example, one significant factor that makes eBay the leading popular online auction site among its competitors is a range of easy means of access and cheap ADR and ODR, for example a feedback system, Square Trade Mediator and eBay's resolution centre for not received items, not as described items and unpaid items.[42] EBay has recognised that disputing parties prefer to adopt private systems of dispute resolution rather than the traditional court system. This is where the law of eBay emerged and has made a huge impact on disputing parties, as many scholars have taken the view that they were "in the shadow of eBay law", rather than the shadow of any other law.[43]

Furthermore, insurance can be used as a mean of building trust in electronic commerce.[44] Tang et al., suggested an interesting approach consisting of specific insurance policies to cover three types of trust in electronic commerce, namely: (1)

---

[41] ADR is the legal method by which legal conflicts and disputes are resolved privately and by means other than through litigation in the courts, usually through mediations or arbitration. ODR is an ADR system in an online environment; See Jeffrey H. Matsuura, *Security, Rights and Liabilties in E-Commerce* (Artech House, INC. 2002) 165-167; Maurice Schellekens and Leo Van Der Wees, 'ADR and ODR in Electronic Commerce' in J.E.J. Prins and others (eds), *Trust in Electronic Commerce : The Role of Trust from a Legal an Organisational and a Technical Point of View* (Kluwer Law International 2002); Egger (n2) 37.

[42] The eBay feedback system is an open forum where eBayers can leave a comment about their experience and rate those whom they buy or sell from under three options, namely Positive, Negative or Neutral Feedback. This will warn other users of potentially troublesome clients and praise good transactions as a reward. Available at < http://pages.ebay.co.uk/help/policies/feedback-ov.html > accessed 1 October 2017;
Square Trade is eBay's preferred dispute resolution provider and it offers two services: a free web-based forum which allows users to attempt to resolve their differences on their own or, if necessary, the use of a professional mediator. Available at <http://pages.ebay.com/services/buyandsell/disputeres.html> accessed 1 October 2017;
Ebay's resolution centre will encourage its members to communicate with each other when there is a problem with a transaction. Available at < http://pages.ebay.co.uk/help/tp/problems-dispute-resolution.html > accessed 1 October 2017;
Lilian Edwards and Ashley Theunissen, 'Creating Trust and Satisfaction Online: How Important Is ADR? The UK eBay Experience' (21st BILETA Conference: Globalisation and Harmonisation in Technology Law, Malta, April 2006) 4-6.

[43] Ethan Katsh, Janet Rifkin and Alan Gaitenby, 'E-Commerce, E-Disputes, and E-Dispute Resolution: In the Shadow of "eBay Law"' (2000) 15 Ohio State Journal on Dispute Resolution 705, 728.

[44] George Yee, 'Buidling Consumer Trust for Internet E-Commerce' in Ronggong Song, Larry Korba and George Yee (eds), *Trust in E-Services: Technologies, Practices and Challenges: Technologies, Practices and Challenges* (Idea Group Inc. 2007) 230.

marketspace trust - trust that both the buyer and the seller must have in the marketspace where the transaction will occur; (2) *buyer's trust* - trust that the buyer has that the goods will be delivered as agreed; (3) *seller's trust*- trust that the seller has that he or she will be paid for delivered goods. They proposed a Comprehensive Marketspace Policy, including Website Security insurance, Error and Omission Content insurance and Trading Partner Identity insurance to resolve the marketspace trust issue, and they proposed a Comprehensive Guaranteed Delivery Policy to cover sellers' trust, and, finally, they suggested a Comprehensive Guaranteed Payment Policy to deal with buyers' trust.[45]

Lastly, legislation also plays an important role in establishing trust in an online market as an external institution for enforcing parties' expectations.[46] Such assurance in the case of legal security of electronic transactions, which are covered by many areas of law, such as contract law and intellectual property law, can provide confidence.[47] However, with an online environment always presenting challenges for law enforcement, extra legal, or "soft law", approaches may also be useful for guaranteeing the trustworthiness of online vendors, for example third-party trustmarks, such as the TrustArc (formally known as TRUSTe) privacy seal.[48]

1.5 An Analysis of the Concept of Trust

By looking at the above multidisciplinary analysis of trust, it can be clearly seen that an exact concept of trust is difficult to define. This is because it can be perceived differently depending on various relationships, circumstances or perspectives, so that a common description of trust remains absent. However, there are some shared elements that can be identified:

(a) Trust is a belief, expectation, willingness, attitude and prediction about ***a***

[45] Fang-Fang Tang and others, 'Using Insurance to Create Trust on the Internet' (2003) 46 Communication of the ACM 337.
[46] Justin (Gus) Hurwitz, 'Trust and Online Interaction' (2013) 161 U Pa L Rev 1579, 1598.
[47] Ronald De Bruin, *Consumer Trust in Electronic Commerce: Time for Best Practice* (Kluwer Law International 2002) 9.
[48] Seal of Approval plays a critical role as a privacy, security or trustworthiness validation, but the effectiveness of this seal is still questionable because users would significantly trust in a seal of their local users' association. See Egger (n2) 12; TrustArc < https://www.trustarc.com/privacy-certification-standards/ > accessed 1 March 2018. See more details in chapter 5.

future event/state between exchange parties.[49] It is a willingness to be ***vulnerable*** to the action of another party based on the expectation that the other will perform a particular action important to the actor, irrespective of the ability to monitor or control that other party.[50] Trust is vested in people or objects humanly created rather than natural events.[51] Rotter claimed that 'trust is a generalised expectancy of the word, promise, oral or written statement of another individual or group'.[52] Trust is based on values varying across individuals, contexts and times.

(b) Trust is only used in ***uncertain and risky situations,*** where there will be an unambiguous course of action in the future, or where the outcome depends on the behaviour of another party, or when the strength of a harmful event is greater than a beneficial event.[53] Luhmann viewed that trust is only required in a situation in which a bad outcome would make you regret your action.[54] However, the risk needs to remain within acceptable limits and these can be evaluated.

(c) On the other hand, trust is only possible to build in a ***familiar world***. It can only be established by a reliable background, including prior knowledge, experience and previous engagement.[55] Moreover, personal information about the trustee is also important in judging trustworthiness, such as knowledge, expertise and reputation.[56] Bateson believes that, when familiarity grows, people come to sense the reliability of each other.[57]

(d) Trust is ***difficult to build, but easy to lose***. Once trust is broken, it is very

---

[49] Cristiano Castelfranchi and Rino Falcone, *Trust Theory: A Socio-Cognitive and Computational Model* (John Wiley & Sons, Ltd., Publication 2010) 44.
[50] Christine Moorman, Rohit Deshpandé and Gerald Zaltman, 'Factors Affecting Trust in Market Research Relationships' (1993) 57 JM 81, 82; Roger C. Mayer, Jame H. Devis and F. David Schoorman, 'An Integrative Model of Organisational Trust ' (1995) 20 AMR 709, 712.
[51] Piotr Sztompka, *Trust: A Sociological Theory* (Cambridge University Press 1999) 19-21.
[52] See generally in Julian B. Rotter, 'Interpersonal Trust, Trustworthiness, and Gullibility.' (1980) 35 Am Psychol 1.
[53] Morton Deutsch, 'Trust, Trustworthiness and the F Scale' (1960) 6(1) J Abnorm and Soc Psych 138.
[54] Luhmann (n3) 99.
[55] Niklas Luhmann, *Trust and Power*, vol 3 (John Wiley & Sons Ltd 1979) 20.
[56] Richard G. Peters, Vincent T. Covello and David B. McCallum, *The Determinants of Trust and Credibility in Environmental Risk Communication: An Empirical Study* (Risk Analysis, 17(1) 43-54, 1997), 45-46.
[57] Patrick Bateson, 'The Biological Evolution of Cooperation and Trust' in Diego Gambetta (ed), *Trust : Making and Breaking Cooperative* (Basil Blackwell 1988) 28.

difficult to rebuild it to its previous state, and sometimes it may never be regained.[58] Lack of trust could destroy a relationship.[59]

As well as that, trust should be distinguished from some other notions, such as faith and confidence. Although they are similar in meaning to trust, the differences are important. In terms of faith, while trust is used to rationalise people's decisions in a situation where there is an *incomplete evidence*, faith comes into play where there is *no evidence*.[60] In terms of confidence, trust maintains interaction in the absence of knowledge, but confidence always rests upon knowledge and a certain amount of evidence.[61]

2. TRUST IN CLOUD COMPUTING

In the aforementioned, I have considered the concept of trust abstract to the perspective of multiple disciplines. In this section, I concentrate, in detail, on how the concept of trust applies specifically to cloud computing. Trust in cloud computing has been receiving special attention from the public over the past few years, especially following the PRISM scandal. Since then, many surveys have shown that some cloud users have become hesitant about placing their data in the cloud, due to their lack of trust in it.[62]

When considering what can weaken users' trust in cloud computing, the answer may involve numerous issues, e.g. the lack of control over data or the threat to data security or privacy. This thesis, however, focuses only on the privacy risks posed by the two legal problems relating to data protection (DP): first, problems regarding application of the EU DP law to the personal data processing in the cloud, and second, problems regarding the relevant EU and US legal frameworks governing access to personal data held in cloud computing for preserving the privacy of individuals in the context of law enforcement and national security. These privacy risks will be explored in detail in this thesis with a view to proposing an approach that could promote trust in cloud

[58] Slovic (n20) 45.
[59] George Cvetkovich and E. Ragnar Lofstedt, 'Conclusion: Social Trust, Consolidate and Future Advances' in George Cvetkovich and E. Ragnar Lofstedt (eds), *Social Trust and Risk Management* (Earthscan Publication Ltd. 1999) 166.
[60] WJ, B and A (n2) 17.
[61] Seligman (n14) 391; Russell Hardin, *Trust* (Polity Press 2006) 29.
[62] See empirical evidences in section 2.2.

computing. Prior to analysing how these legal problems affect users' trust in cloud computing in the following chapters, this section will explore the concept of trust in cloud computing.

Firstly, it is necessary to describe the three key actors who will be involved in trust in cloud computing. They are as follows:

(a) Cloud Users are those who adopt cloud services by placing data into the cloud.

(b) Cloud Service Providers (CSPs) are those with whom cloud users' data is being entrusted. Several CSPs who provide different kinds of service will have different abilities to control each component of the cloud infrastructure.[63]

(c) Referees are third parties who conduct independent assessments and provide recommendations regarding the trustworthiness of several CSPs in relation to particular issues, for example TrustArc Privacy Certification Standard or Skyhigh Enterprise – Ready Seal.[64]

2.1 Key Definitions of Trust in Cloud Computing

Although the issue of trust in cloud computing has been discussed by a range of scholars, only a few descriptions of trust in cloud computing are provided as follows:

Noor et al., described trust in cloud computing as

> the extent to which a cloud service consumer ***is willing to depend on a CSP***, provisioning a cloud service and expects certain qualities that the CSP promised to be met.[65]

Srinivasan, expressly demonstrated trust in cloud computing as

> a customer is ***willing to use the services of an unknown third party*** to

[63] See more details in chapter 1, section 4.

[64] See (n48); Skyhigh CloudTrust Programme can help cloud users lower their risks and streamline the evaluation process by providing an objective and comprehensive evaluation of a service's security controls and enterprise readiness based on a detailed set of criteria developed in conjunction with the Cloud Security Alliance (CSA).The Skyhigh Enterprise-Ready Seal will be given to those cloud service providers who fully satisfy the most stringent requirements for data protection, identity verification, service security, business practices and legal protection.
See< https://www.skyhighnetworks.com/cloud-trust-program/> accessed 11 November 2017.

[65] Talal H. Noor, Quan Z. Sheng and Athman Bouguettaya, *Trust Management in Cloud Services* (Springer 2014) 13.

> handle all their computing needs. This means that the customer is willing to let their sensitive data reside on a remote server that they do not own.[66]

Huang and Nicol, described trust in cloud computing as

> a mental state comprising (1) ***expectancy*** – the trustor expects a specific behaviour from the trustee; (2) ***belief*** – the trustor believes that the expected behaviour occurs, based on the evidence of the trustee's competence, integrity and goodwill; (3) ***willingness to take risk*** – the trustor is willing to take risk for that belief.[67]

Van de Werff et al., adopted the description of trust in cloud computing as

> three state processes consisting of the forming of ***positive expectation***, the decision to make oneself ***vulnerable to another party and a risk taking act***.[68]

These definitions do not differ greatly from general concepts of trust discussed above. If we apply general characteristics of trust from A to D in Section 1.5 to cloud computing, some particular issues regarding trust in cloud computing will emerge, as follows:

(a) Cloud computing is clearly only viable if cloud users are willing to make themselves vulnerable by allowing their data to reside in the cloud, which they do not own, and allowing it to be controlled by CSPs, despite the fact that such providers may act in ways that can have a negative impact on cloud users.[69]

(b) Since cloud computing can present a variety of risks and uncertainties for cloud users, cloud computing has to be based on the strong expectation of cloud users that the CSP will perform actions that will result in a positive outcome for them.

(c) The best circumstance that can facilitate trust in cloud computing is considered to be the state of familiarity.[70] Familiarity canonically needs history as a reliable

---

[66] S. Srinivasan, 'Building Trust in Cloud Computing: Challenges in the Midst of Outrages' (2014) Proceedings of Information Science & IT Education Conference 305, 307.
[67] Jingwei Huang and David M Nicol, 'Trust Mechanisms for Cloud Computing' (2013) 2 JoCCASA 1, 2.
[68] Lisa Van Der Werff and others, *Building Trust in the Cloud Environment: Towards a Consumer Cloud Trust Label* (ICDS 2014: The Eighth International Conference on Digital Society), 158.
[69] Srinivasan (n66) 307-8.
[70] Luhmann, *Trust and Power* (n55) 19-20.

background for absorbing the complexity, risk and uncertainty.[71] Users, however, do not build up familiarity of the real world with online cloud services: they may use cloud services one time or many times, but they will not meet the providers in real life, and they have little information to hand about the providers, other than lengthy and unread contracts, and they will have little or no knowledge about who, if anyone, provides *delegated* cloud services, for example infrastructure, storage and software services. How, then, can familiarity be provided, or be substituted? Experience in electronic commerce, generally, especially Consumer to Consumer (C2C) electronic commerce, is the answer, which lies in a combination of solutions, such as: a fair contract; the reputation and the brand of service providers; good feedback from satisfied users as a way of packaging reputation; good dispute resolution mechanisms, including ADR and ODR; industry trustmarks; effective regulations in relation to cloud computing; and regulators who are easy to access and have effective sanctions.[72]

(d) Once trust in cloud computing has been broken, it is quite difficult to be rebuilt, as was seen after the revelations of the PRISM scandal in 2013. Many surveys have shown that cloud users feel reluctant about adopting a cloud service, due to their trust being negatively affected by the privacy risks brought about by cloud services.[73]

Accordingly, many US controlled CSPs, such as IBM and Google, who may have suffered from a decrease in profit, have been attempting to restore the trust of EU users by building data centres within the EU, in order to keep their EU users' data away from the US NSA.[74]

Especially after the Cambridge Analytica revelation in 2018, which revealed that Cambridge Analytica, a British political consulting firm, had been obtaining access to the personal data of about 87 million Facebook users without their permissions since 2015 (through third-party applications that were allowed by Facebook to collect the

[71] ibid.
[72] Noll (n40), 209-210.
[73] See empirical evidence in section 2.2.
[74] IBM, 'IBM Opens First Cloud Data Center With SoftLayer in Germany' 7 January 2015 <http://www-03.ibm.com/press/us/en/pressrelease/45786.wss> accessed 11 July 2017; Glyn Moody, 'Microsoft Building Data Centers in Germany that US Government Can't Touch' 12 November 2015 <http://arstechnica.com/information-technology/2015/11/microsoft-is-building-data-centres-in-germany-that-the-us-government-cant-touch/> accessed 11 January 2016.

personal data of Facebook users for only academic use) for targeting potential Trump voters during the 2016 presidential election, users' trust seem to be reduced by this scandal.[75] This decline of users' trust then led to a collapse of Facebook's market values in 2018.[76] It is likely that the Facebook loss of EU users is as much down to the GDPR re-consenting as it is to the Cambridge Analytica fallout. Facebook is, thus, now changing the way in which it shares data with third party applications, in order to regain users' trust.[77]

As trust in cloud computing is a dynamic process and it cannot be established overnight, a more stringent approach needs to be put in place with a view to making users feel confident enough to rely on cloud services, such as a change in the US law or a stronger oversight regime for preserving individuals' privacy.[78]

2.2 Do Individuals and SMEs Trust Cloud Computing?

Cloud computing is becoming increasingly popular among a large number of EU users. The obvious reason for cloud adoption lies in a number of advantages offered by cloud computing, such as lower costs, better scalability, improved flexibility and various kinds of services.[79]

Nevertheless, there remain some doubts regarding the correlation between users' trust in cloud computing and the adoption of cloud computing. In terms of the theory of trust discussed above, the situation of trust is when individuals are willing to be vulnerable in a risky and uncertain situation in exchange for various associated

---

[75] Binns A, 'Cambridge Analytica Scandal: Facebook's User Engagement and Trust Decline' (*28 March 2018*) <http://theconversation.com/cambridge-analytica-scandal-facebooks-user-engagement-and-trust-decline-93814> accessed 1 June 2018.

[76] Vogelstein F, 'Facebook Just Learned the True Cost of Fixing its Problems' (*25 July 2018*) <https://www.wired.com/story/facebook-just-learned-the-true-cost-of-fixing-its-problems/> accessed 25 July 2018.

[77] Wong JC, 'Mark Zuckerberg Apologises for Facebook's 'Mistakes' over Cambridge Analytica' 22 March 2018 <https://www.theguardian.com/technology/2018/mar/21/mark-zuckerberg-response-facebook-cambridge-analytica> accessed 1 June 2018.

[78] Andrew Orlowski, 'No Change in US Law, No Data Transfer Deals – German State DPA' 15 October 2015<http://www.theregister.co.uk/2015/10/15/data_protection_safe_harbor_schrems_facebook/> accessed 11 January 2016; A29WP, *Opinion 04/2014 on Surveillance of Electronic Communications for Intelligence and National Security Purposes* (819/14/EN WP 215, Adopted on 10 April 2014). See more details in chapter 4.

[79] See advantages of cloud computing in chapter 1, section 5.

advantages.

This leads to the question of whether cloud users realise that there might be some associated risks, such as risks regarding privacy or data security. If the answer is 'yes', then the question arises as to whether or not they will make use of cloud computing. If they decide to adopt cloud services, is this simply because of its range of benefits, or because of their trust in cloud computing, or could it be something else entirely? This section will attempt to answer all of these questions.

Since the emergence of cloud computing in 2008, it has come a long way in just a few years. Cloud computing has been widely adopted by various sectors, including individuals, businesses and public organisations. Many surveys have shown that cloud computing's adoption grew quickly between 2008-2012.[80] In 2010, the survey of the European Union Agency of European Network and Information Security (ENISA) presented that the majority of SMEs (73%) based in the EU were willing to outsource to multiple CSPs,[81] and, in 2012, the surveys carried out in nine European Countries, including the United Kingdom (UK), Poland, Sweden, Spain, Hungary, Italy, Germany, France and the Czech Republic, by the International Data Corporation (IDC) showed that the vast majority of EU citizens (64%) had adopted at least one type of cloud service.[82]

However, the risks and uncertainties still cast doubt on cloud computing. In 2010, the report of the Cloud Security Alliance (CSA) pointed out seven top threats of cloud computing, namely (1) the abuse and nefarious use of cloud computing; (2) insecure application programming interfaces; (3) malicious insiders; (4) shared technology vulnerabilities; (5) data loss or leakages; (6) account, service and traffic hijacking; and

[80] See Mimecast, 'Cloud Computing Adoption Survey' 2010 <https://system.netsuite.com/core/media/media.nl?id=181214&c=601905&h=2ef3796f7c4d9c8a585e&_xt=.pdf> accessed 1 July 2017, 2; Vivek Kundra, 'Federal Cloud Computing Strategy' The White House Washington, 8 February 2011 <https://www.dhs.gov/sites/default/files/publications/digital-strategy/federal-cloud-computing-strategy.pdf> accessed 1 May 2017.
[81] ENISA, An SME Perspective on Cloud Computing: Survey (June 2010) 11.
[82] IDC, 'Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Up-take' SMART 2011/0045, 13 July 2012 <http://cordis.europa.eu/fp7/ict/ssai/docs/study45-d2-interim-report.pdf> accessed 1 May 2017, 10.

(7) unknown risk profiles.[83] The study of the ENISA in 2012 demonstrated that three main aspects of risks are posed by cloud computing, namely risks relating to costs, risks relating to legal and regulatory issues and risks affecting data confidentiality, integrity and availability.[84]

It can be seen that all these risks have been widely recognised by individuals (who are concerned about their privacy) and SMEs (who are concerned about the privacy of their customers) as cloud users. In 2010, the worldwide surveys interviewing individual cloud users in Germany and the UK, carried out by Fujitsu, presented that 88% of individual users were worried about who had access to their personal data residing in the cloud.[85] The ENISA's surveys in 2010 stated that the privacy and availability of the services and/or data were the most concerning issues of the EU SMEs when deciding whether or not to adopt cloud services.[86] A survey conducted in the UK showed that, in 2012, SMEs were interested in exploiting cloud services, although there were still some concerns about data security and privacy.[87] According to the IDC surveys in 2012, 43% of EU individual cloud users do have major concerns about security, data location and data privacy.[88]

Nevertheless, these users' concerns did not seem to slow down, or impede, the use of cloud computing. When considering why individuals and SMEs still choose to use cloud computing, the main reason seems to be the perceived usefulness of cloud computing for cloud users.[89] The familiar factors of cheapness, scalability, flexibility, etc. have considerable influence on the intention of both individuals and SMEs (who are

---

[83] Cloud Security Alliance, 'Top Threats to Cloud Computing Report (Ver.1.0)' 2010 <https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf> accessed 1 March 2015, 6.
[84] ENISA, *Consumerization of IT: Top Risks and Opportunities : Responding to the Evolving Threat Environment* (2012) 9-13.
[85] Fujitsu Research Institute, 'Personal Data in the Cloud: A Global Survey of Consumer Attitudes' Technical Report, 2010 <http://www.fujitsu.com/downloads/SOL/fai/reports/fujitsu_personal-data-in-the-cloud.pdf> accessed 1 July 2017, 5.
[86] ENISA, An SME Perspective on Cloud Computing : Survey (n81).
[87] Sahandi R, Alkhali A and Opara-Martins J, *SMEs' Perception of Cloud Computing: Potential and Security* (Collaborative Networks in the Internet of Service, Working Conference on Virtue Enterprise, 2012).
[88] See IDC (n82) 27.
[89] Paul Ambrose and Ananth Chiravuri, 'An Empirical Investigation of Cloud Computing for Personal Use' (2010) 24 MWAIS 2010 Proceedings 1, 2-3.

too small to have their own facilities) to adopt cloud services.[90] Furthermore, the most frequently used cloud services among these users are free services (e.g. Yahoo, Facebook) or low-cost services (e.g. Dropbox), and they may decide to ignore the possible risks associated with cloud computing for the sake of taking advantage of it. All of these circumstances probably fall within the situation of trust, as discussed in the previous section, where users decide to make themselves vulnerable to risk taking acts in exchange for embracing the benefits of cloud computing. However, it should be noted that there is, as yet, no explicit evidence showing a direct link between trust in cloud computing and cloud computing adoption.

The issue of trust in cloud computing has become a critical subject that has received special attention from researchers, after the disclosure of the US NSA's electronic surveillance in 2013.[91] The Snowden revelations may yet prove to be a tipping point in how willing users are to place their trust in cloud computing. It has been found in a number of empirical studies that a number of risks and uncertainties created by cloud computing do affect users' trust in cloud computing and this situation is having an influence on the uptake of cloud computing by individuals and SMEs as cloud users. The research carried out by scholars from the Oulu University of Applied Sciences, Finland found that the important factor behind the adoption of cloud computing in SMEs is the level of trust in CSPs.[92] As can be seen following the disclosure of the US NSA's electronic surveillance programs, the US cloud company lost $22 to $35 billions because the EU users hesitate to engage with it.[93] The privacy concerns of cloud users seem to reduce the level of trust in cloud computing, which then prevents SMEs from using cloud computing.

---

[90] ENISA, 'Cloud Computing : Benefits, Risks And Recommendations for Information Security' December 2012 <https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security> accessed 1 June 2017 5-6; Anca Apostu and others, 'Study on Advantages and Disadvantages of Cloud Computing - The Advantages of Telemetry Applications in the Cloud' (2013) Applied Computer Science 113, 119.

[91] See more details in chapter 4.

[92] Mikkonen I, *Cloud Computing – SME Company Point of View* (8th International Research Conference Management Challenges in the 21st Century, Bratislava, April 12, 2016).

[93] Castro D, *How Much Will PRISM Cost the U.S. Cloud Computing Industry?* (The Information Technology Innovation Foundation Project, August 2013).

Furthermore, the report of Information Technology & Innovation Foundation in 2013, showed that after the Snowden revelations 10% of individual users outside the US cancelled their contracts with US-based CSPs and 56% would be "less likely" to adopt a US-based cloud computing service.[94] The surveys carried out by the UK Digital Catapult Centre in 2014 presented that more than a quarter of UK individual online users do not trust online service providers with regard to their personal data, as they are concerned that their data will not be used responsibly.[95] Regarding the EuroState statistics on SMEs' use of cloud computing in the EU in 2014 and 2016, the risk of a security breach is the key reason for SMEs not using cloud computing.[96] The Accenture Digital Consumer Survey conducted in 2014, with 24,000 users in 24 countries, including the UK, Spain, Sweden and Italy, demonstrated that 54% of individual online users were cautious about sharing their personal data on the internet, due to their lack of trust in data security.[97]

The Eurobarometer survey, interviewing 28,000 EU individuals in March 2015, showed that the respondents were concerned about the security of their personal data, especially in the case of a mass data collection by governments. They feel uncomfortable about entrusting their personal data to CSPs, as their trust has been disrupted by the PRISM scandal.[98] In 2017, a new report from Yoti and YouGov, which surveyed over 2,000 individual online users in the UK, indicated that the majority of the respondents, being 87 %, are worried about the security of their personal data when sharing it online and they do not trust how online service providers protect and secure

[94] The Information Technology & Innovation Foundation, 'How Much Will PRISM Cost the U.S. Cloud Computing Industry?' August 2013 <http://www2.itif.org/2013-cloud-computing-costs.pdf> accessed 1 June 2017, 3; Charles Authur, 'Fears Over NSA Surveillance Revelations Endanger US Cloud Computing Industry' The Guardian, 8 August 2013 <http://www.theguardian.com/world/2013/aug/08/nsa-revelations-fears-cloud-computing> accessed 1 July 2017.

[95] Digital Catapult Centre, 'Trust in Personal Data : A UK Review' 2014 <http://www.digitalcatapultcentre.org.uk/wp-content/uploads/2015/07/Trust-in-Personal-Data-A-UK-Review.pdf> accessed 1 January 2016, 5.

[96] Eurostat, Cloud Computing - Statistics on the Use by Enterprises (2014).

[97] Accenture, 'Digital Trust in IoT Era' 2015 <https://www.accenture.com/t20160318T035041__w__/us-en/_acnmedia/Accenture/Conversion-Assets/LandingPage/Documents/3/Accenture-3-LT-3-Digital-Trust-IoT-Era.pdf> accessed 1 May 2017, 6.

[98] Commission, 'Data Protection Eurobarometer: Fact Sheet' June 2015 <http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_eurobarometer_240615_en.pdf> accessed 1 May 2017, 1-3.

their personal data.[99]

Apart from that after the recent disclosure of the Cambridge Analytica scandal, global surveys of 3,000 people conducted by the Ponemon Institute in April 2018, an independent research institute specialising in privacy and DP, showed that users' trust in Facebook had dropped by 66%.[100] Facebook admitted that the rate of monthly average users in Europe slightly fell and this is partly due to the Cambridge Analytica data breach.[101] This situation then led to the collapse of Facebook's share price by more than $119 billion, as a result of the decline of users' trust.[102]

As a result of all these empirical evidence, it can be concluded that the privacy concerns do in fact have business costs in term of decrease the level of trust in cloud computing of users in the market. The EU individuals and SMEs thus arguably do not fully trust cloud computing, as they cannot be sure about the privacy protection and security of the data held in the cloud and this lack of trust seems to affect their adoption of cloud computing, at least to some extent.[103] It can be said that the uptake of cloud computing and trust in cloud computing are somehow linked.

2.3 Criteria for Creating Trust in Cloud Computing

---

[99] YouGov United Kingdom and Yoti, 'British Opinions on Identity and Personal Information' 2017 <https://get.yoti.com/yougov-results/yougov-report-2/> accessed 1 May 2017.

[100] It was found that the Cambridge Analytica used personal information harvested from more than 50 million Facebook users without their permission to build system that could target US voters with personalised political advertisements based on their psychological profile. See Meredith S, 'Facebook-Cambridge Analytica: A Timeline of the Data Hijacking Scandal' <https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html> accessed 1 May 2018; Weisbaum H, 'Trust in Facebook has Dropped by 66 Percent since the Cambridge Analytica Scandal' (*19 April 2018*) <https://www.nbcnews.com/business/consumer/trust-facebook-has-dropped-51-percent-cambridge-analytica-scandal-n867011> accessed 1 June 2018

[101] Vogelstein F, 'Facebook Just Learned the True Cost of Fixing its Problems' (*25 July 2018*) <https://www.wired.com/story/facebook-just-learned-the-true-cost-of-fixing-its-problems/> accessed 25 July 2018; Morin C, 'Facebook See Users Decline in Europe Amid GDPR and Cambridge Analytica Fall Out ' (*25 July 2018*) <http://adage.com/article/digital/facebook-sees-users-flee-europe-gdpr-effect/314384/> accessed 26 July 2018.

[102] Neate R, 'Over $119bn Wiped off Facebook's Market Cap After Growth Shock' (*26 July 2018*) <https://www.theguardian.com/technology/2018/jul/26/facebook-market-cap-falls-109bn-dollars-after-growth-shock?CMP=Share_AndroidApp_Gmail> accessed 26 July 2018.

[103] See generally in EY, 'Corporate Misconduct — Individual Consequences Global Enforcement Focuses the Spotlight on Executive Integrity 14th Global Fraud Survey' 2016 <http://www.ey.com/Publication/vwLUAssets/ey-global-fraud-survey-2016/$FILE/ey-global-fraud-survey-final.pdf> accessed 1 May 2017.

As this thesis aims to provide approaches for making cloud computing a trustworthy service, it is important to determine what makes individuals and SMEs either trust or distrust cloud computing. Regarding the empirical evidence provided in Section 2.2, there are a range of issues that directly affect users' trust in cloud computing, which could be categorised into three main concepts, as follows:[104]

2.3.1 Transparency and Control

This is the state where CSPs provide cloud users with all of the information relating to their data and also provide such users with the capabilities to decide, track and audit how and where the data is being used, by whom and for what purposes.

Transparency has been receiving considerable attention across several domains as a universal remedy for all sorts of socioeconomic, sociocultural, socio-political and civic problems.[105] It is considered to be a self-interested exercise of power. As Brandeis said '[s]unlight is said to be the best of disinfections; electronic light the most efficient policemen'.[106] Transparency is one of the key obligations required by the EU DP law, for example, in the form of subject access rights and the notification principle.[107] It is a critical mechanism for dealing with DP issues, as the data residing in the cloud might be compromised by the CSPs to whom they entrust their data or by other sub-CSPs, or sub-sub CSPs, and it is not easy for cloud users to take full control over their data. Transparency could make cloud users feel that they are still able to exercise control over

[104] There is now an entire field called Fairness, Accountability and Transparency (FTA) in relation to algorithmic processing, which is often something delivered via cloud computing. There is also an annual FTA conference dedicated to bringing together a diverse community to investigate and tackle issues relating to the topics of fairness, accountability, transparency, ethics and interpretability in machine learning, recommender systems, the web and other technical disciplines. These three factors for creating and evaluating trust in cloud computing provided in this thesis have been, at least, developed independently but come to much the same kind of conclusion as the FTA project. See <https://fatconference.org/index.html> accessed 1 July 2018.

[105] Jaydip Sen, 'Security and Privacy Issues in Cloud Computing' in Ruiz Martinez, Pereniguez Garcia and Marin Lopez (eds), *Architectures and Protocols for Secure Information Technology; Information Science Reference: Hershey, PA, USA* (IGI Global 2013) 17; Zarsky T, 'Transparency in Data Mining : From Theory to Practice ' in Custer B and others (eds), *Discrimination and Privacy in the Information Society* (Springer 2013) 301-324.

[106] Louis Brandeis, *Other People's Money, and How Banker Use It* (National Home Library Foundation, 1933), 62.

[107] See more details in chapter 3.

their data, thus enabling users to make an informed decision with regard to adopting cloud computing.

Furthermore, as transparency has always have intimately linked to the idea of control of decision making under uncertain situations, the loss of control over data may also affect users' trust in cloud computing.[108] Therefore, whether or not individuals trust cloud computing does seem to depend on how much transparency there is in relation to their data, as it is served by CSPs.

2.3.2 Accountability

This is a state where CSPs take responsibility for the stewardship of the data held in the cloud according to contractual and legal requirements and where CSPs can demonstrate their compliance to their users and auditors. It goes far beyond merely responsibility by obligating CSPs to be answerable for all their actions and to be liable, and to provide remedies, for any damages resulting from their non-compliance.

Accountability is a common term used in computer science, finance and public governance.[109] Accountability has also been associated with the concept of privacy and DP, and is a critical principle enshrined in the EU DP law.[110] The "accountability gap" is one of the causes of what is conceived as being regulatory failure, lack of faith in the regulatory framework amongst the general public and the low priority of DP compliance.[111]

Accountability could be used to deal with risks and uncertainties brought about by cloud computing.[112] In this case, CSPs should be clear about how to deliver their services to users, how to manage users' data and how to detect, prevent and control risks

[108] Umar Mukhtar Ismail and others, 'A Framework for Security Transparency in Cloud Computing' (2016) 8 Future Internet 1, 4-5.
[109] Siani Pearson and others, *Accountability for Cloud and Other Future Internet Services* (IEEE 4th International Conference on Cloud Computing Technology and Science, 2012) 630.
[110] See more details in chapter 3.
[111] Nick Papanikolaou, Siani Pearson and Nick Wainwrigh, *Accountability in Cloud Computing* (Building International Cooperation for Trustworthy Discussion Paper, 22 June 2011) 2.
[112] See generally in W Kuan Hon and others, *Cloud Accountability: The Likely Impact of the Proposed EU Data Protection Regulation* (Tilburg Law School Legal Studies Research Paper Series, No 07/2014).

and what they will do when, and if, damages occur.[113] The accountability of CSPs would play a critical role in the process of making the decision as to whether or not to trust cloud computing, because it empowers users to make informed choices about selecting a provider based on a solid understanding of the consequences of their choice. [114]

2.3.3 Data Security

This is the state in which the data of cloud users is free from breach, due to the fact that CSPs employ necessary security measures for preserving the confidentiality, availability and integrity of data and to comply with cloud contracts and relevant legal obligations.

Data security is seen to be the combination of preservation of confidentiality, integrity and availability of information.[115] It is also a critical obligation imposed by the EU DP law (requiring both the data controller and data processor to adopt appropriate technical and organisational measures against any occurrence of potential damage to the data) to preserve the privacy of data subjects.[116] Security and privacy are not the same, but many scholars treat these two as interchangeable, or as inextricably intertwined.[117] Swire and Lauren viewed that, while the goal of security is to stop unauthorized access, the goal for privacy is to define what is treated as unauthorised.[118]

There are two main concepts of data security issues in the cloud, including (1) a threat, which is a potential attack that may lead to misuse of data or resources; and (2) vulnerability, which refers to the flaws in a system that allow an attack, or harm, to be successful.[119] The complexity of features of cloud computing, such as shared multi-tenant environment, distributed, heterogeneous and virtualized resources, is likely to

---

[113] See generally in R. Ko, Lee B.S. and S. Pearson, 'Towards Achieving Accountability, Auditability and Trust in Cloud Computing' in A. Abraham and others (eds), *Advances in Computing and Communications* (ACC 2011. Communications in Computer and Information Science, vol 193. Springer, Berlin, Heidelberg 2011).

[114] See generally in Gilje Jaatun M and others, 'Enhancing Accountability in the Cloud' [2016] IJIM 1.

[115] ISO: 27001: Information Security Management – Specification with Guidance for Use, London (2005).

[116] See more details in chapter 3.

[117] See generally in Bambauer DE, 'Privacy Versus Security' (2013) 103 JCLC 667; Nissenbaum H, *Privacy in Context : Technology, Policy and the Integrity of Social Life* (Stanford University Press 2010).

[118] See more details in Swire P and Steinfeld L, 'Security and Privacy After September 11: The Health Care Example' (2002) 86 Minn L Rev 1515, 1522.

[119] Algirdas Avizienis and others, 'Basic Concepts and Taxonomy of Dependable and Secure Computing' (2004) 1 IEEE Transactions on Dependable and Secure Computing 11, 3-5.

create a number of risks to the security of users' data held in the cloud, such as in cases of it being misused, lost, damaged or disclosed to a third party.[120] Data security in the cloud has been perceived to be more complicated than data security in traditional information systems.[121] Therefore, data security is always a major concern of cloud users, and would probably have a direct impact on users' trust in cloud computing.[122]

Regarding the three main criteria discussed above, it can be seen that the breaking down of at least one of these criteria would create risks associated with the privacy of cloud users and this situation would likely weaken users' trust in cloud computing. As this thesis aims to determine potential approaches that could be used for rebuilding trust in cloud computing after it has been disrupted by the two legal problems relating to DP, these criteria will play a critical role when examining the circumstances in which trust in cloud computing could develop.[123] Achieving all of these criteria would be helpful for enhancing the possibility of users placing their trust in the cloud.

CONCLUSIONS

Trust has played quite a critical role in the cloud, in which there is a high possibility of risks and uncertainties, as it can either facilitate or prevent individuals from engaging with cloud computing. Trust in cloud computing is perceived as *the willingness to adopt cloud services by letting the data reside on remote servers that are controlled by others*.

Trust makes relationships between CSPs and cloud users possible. As cloud computing does leave users exposed and vulnerable in some ways, trust can be used as a

[120] See generally in Diogo A.B. Fernandes and others, 'Security Issues in Cloud Environments: A Survey' (2013) 13 INT J INF SECUR 113; Keiko Hashizume and others, 'An Analysis of Security Issues for Cloud Computing' (2013) 4 JISA 1, 2-4.

[121] Sun Yunchuan and others, 'Data Security and Privacy in Cloud Computing' (2014) IJDSN 1, 2.

[122] Trend Micro, 'Cloud Security Survey Global Executive Summary ' August 2012 <http://www.trendmicro.com/cloud-content/us/pdfs/about/2012_global_cloud_security_survey_executive_summary.pdf> accessed 11 February 2016; Siani Pearson, 'Privacy, Security and Trust in Cloud Computing' in Siani Pearson and George Yee (eds), *Privacy and Security for Cloud Computing* (Springer 2013) 11.

[123] See generally in Ayesha Kanwal and others, *Assessment Criteria for Trust Models in Cloud Computing* (2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing 2013).

kind of glue to hold together the cloud/user relationship.[124] Trust will help potential users to overcome the hindrances by persuading them to expose themselves to those risks and uncertainties for the sake of taking advantage of cloud computing.[125] In addition, trust can create values that enable relationships between CSPs and cloud users to function sustainably over the long term, and to flourish.[126]

According to empirical evidence from various sources, there seem to be a correlation between the level of trust in cloud computing and the adoption rate of cloud computing, at least to some extent. Especially after the Snowden revelations, surveys explicitly showed that individuals and SMEs do hesitate to adopt cloud services, due to their lack of trust in them. This is because the range of uncertainties and risks posed by cloud computing do affect the three factors, including: (1) transparency and control; (2) accountability; and (3) data security, that are very important for maintaining users' trust in cloud computing.

As a result, addressing the existing problems that create risks and uncertainties for cloud users and implementing appropriate measures that would achieve all of the three factors to make cloud computing trustworthy among users, would likely help to facilitate faster use of cloud computing, which could then potentially lead to economic development of the EU and global society as a whole.

The next two chapters will discuss the two key legal problems relating to DP in the cloud that prevent the current legal frameworks from promoting trust in cloud computing. The criteria for creating trust in cloud computing provided in this chapter will be taken into account when analysing how is user trust in cloud computing disrupted by these legal problems and when determining potential solutions to the lack of trust in the cloud, which will be provided in Chapter 5.

---

[124] See generally in Huang and Nicol Felix Meixner and Ricardo Buettner, *Trust as an Integral Part for Success of Cloud Computing* (ICIW 2012 : The Seventh International Conference on Internet and Web Applications and Services 2012).

[125] Sheikh Mahbub Habib and others, 'Trust as a Facilitator in Cloud Computing: A Survey' (2012) 1 JoCCASA 1, 2.

[126] Neil Richard and Woodrow Hartzog, 'Taking Trust Seriously in Privacy Law' (2015) 19 Standford Technology Law Review 431, 435.

CHAPTER 3

LEGAL PROBLEMS REGARDING THE APPLICATION OF THE EU DATA PROTECTION LAW IN CLOUD COMPUTING

INTRODUCTION

As discussed in the previous chapter, the law is one of the major approaches that could be used for enhancing trust in cloud computing. However, the existing legal frameworks covering many areas of law, such as the contract law or DP law, do not seem to be working well in the cloud. This is because the characteristics of cloud computing have troubled the existing legal frameworks at various points. Consequently, trust in cloud computing is likely to be affected by these issues.

This chapter focuses on the DP problems cloud computing creates for both CSPs and cloud users. There are two main sections in this chapter that aim to engage with Research Question D: what legal problems affecting trust in cloud computing emerge from the EU DP law?

Following an introduction, section one considers the EU DP law in relation to two main topics, including (1) DP principles regarding the former EU DP law (Directive 95/46/EC(DPD)); and (2) the EU DP law reform. Then, section two discusses the legal problems involved in applying the DPD to cloud computing, and also provides an analysis of the effectiveness of the changes made by the General Data Protection Regulation (GDPR) in dealing with such legal problems. From this analysis, I conclude that severe problems arise concerning the status of various actors involved in the same set of data processed, the applicable law and the data export rules. Lastly, conclusions will be drawn from the various points discussed in this chapter.

1. EU DATA PROTECTION LAW REGULATING THE PROCESSING OF PERSONAL DATA IN CLOUD COMPUTING

1.1 EU Data Protection Directive 95/46/EC

The DPD, which is now invalid and is replaced by the GDPR, came fully into force on

25 October 1988 and all Member States were obliged to implement this directive in order to set an equivalent level of DP concerning the processing of personal data across the Member States.[1] It was legally binding in the 28 EU Member States and in Iceland, Liechtenstein and Norway (European Economic Area (EEA) Member States).[2]

The DPD was applied to the processing of personal data wholly or partly by automatic means and to the processing other than by automatic means of personal data that formed part of a filing system or was intended to form part of a filing system.[3] However, some types of data processing were exempt from this directive, such as the processing of personal data relating to public security, state security and criminal law.[4]

Each Member State should apply its DP law adopted pursuant to this Directive to the processing of personal data where

(1) the processing was carried out in the context of activities of an establishment of the data controller (controller)on the territory of the Member State;

(2) the controller was not established on the Member State's territory, but in a place where its national law applied by virtue of international public law;

(3) the controller was not established on Community territory and, for the purposes of processing personal data, made use of equipment situated on the territory of the said Member State, unless such equipment was used only for purposes of transit through the territory of the Community.[5]

The DPD imposed fundamental DP rules concerning the processing of personal data, which must be satisfied by the controller as follows:

(1) Personal data must be processed fairly and lawfully (**legitimacy principle**).[6]

(2) Personal data must be collected for specified, explicit and legitimate purposes

[1] DPD, Rec 8.
[2] The list of EEA Member States (29 July 2013), available at < http://ec.europa.eu/eurostat/statistics-explained/index.php/Glossary:European_Economic_Area_(EEA) > accessed 21 May 2018; The EEA countries which are not the EU Member States have to implement the EU DP law. Thus, the word 'EU' is used throughout this thesis as it includes the EEA countries and the word 'non-EU' means the territory outside the EU and the EEA (often known as third countries).
[3] DPD, Art 3(1).
[4] DPD, Art 3(2).
[5] DPD, Arts 4(1)(a) (b) and (c).
[6] DPD, Art 6 (a).

(**purpose limitation principle**).[7]

(3) Personal data must be adequate, relevant and not excessive in relation to the purposes for which the personal data were collected and/or further processed (**adequacy principle**).[8]

(4) Personal data must be accurate and, where necessary, kept up to date (**integrity principle**).[9]

(5) Personal data must be kept in a form of which permits identification of the data subject for no longer than was necessary for the purposes for which the data were collected or for which they were further processed.[10]

There were further legal obligations that were imposed on the controller, as follows:

(1) The controller must provide the data subject with

(a) the identity of the controller;

(b) the purpose of the processing;

(c) any further information such as the recipients (**subject access rights**).[11]

(2) The controller must notify DPA of

(a) the name and address of the controller and any relevant representative;

(b) the purpose of the processing;

(c) a description of the category or categories of persons affected and of the data relating to them;

(d) the recipients or categories of recipients to whom the personal data may be disclosed;

(e) proposed transfers to third countries;

(f) a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken to ensure the security of the processing

[7] DPD, Art 6 (b).
[8] DPD, Art 6 (c).
[9] DPD, Art 6 (d).
[10] DPD, Art 6 (e).
[11] DPD, Arts 10, 11.

(**notification principle**).[12]

(3) The controller must ensure an adequate level of protection of the processing of personal data by implementing the appropriate technical and organisational measures against any kind of potential damage arising to the data, e.g. unauthorised access, unlawful destruction or accidental loss (**security obligation**).[13]

(4) The controller must choose a data processor (processor) who can provide a sufficient guarantee in complying with the appropriate technical and organisational measures against any kind of potential damage when performing the processing of the personal data (**security obligation**).[14]

Unlike the controller, the processor was only required to process the personal data according to the instructions of the controller.[15] Performing such processing must be governed by a contract or a legal act that is binding between the controller and the processor. Therefore, the processor should act only on the basis of this contract.[16]

The DPD, in principle, prohibited the transfer of personal data to third countries, in order to prevent the controller from avoiding the EU DP legal obligations. Nevertheless, with a view to facilitating the free flow of data, the DPD allowed such data transfer under the condition that (1) the third countries can ensure an adequate level of protection approved by the Commission (Article 25(2)); (2) there were specific circumstances, e.g. data subject' consent; or necessary to protect the vital interests of the data subject (Article 26(1)); (3) the data exporter and the third country's data importer have agreed to abide by standard contractual clauses (SCCs)(Article 26(2)).[17]

There were two other legitimate conditions that justified the data transfer to non-EU countries, but were not recognised by the DPD. Firstly, the Binding Corporate Rules (BCRs) were a set of legally binding rules for particular corporate groups, enabling a

[12] DPD, Arts 18, 19.
[13] DPD, Art 17 (1).
[14] DPD, Art 17 (2).
[15] DPD, Art 17 (3).
[16] DPD, Art 17 (3).
[17] DPD, Art 25-26. Regarding the DPD, there were two step-procedures for transferring data to third countries which need to be fulfilled: (i) there must be a legal basis for the lawful processing of the data (Art 7); (ii) there must be a legal basis for transferring personal data to third countries (Art 25 or 26).

multinational organisation to perform international data transfers between its subsidiaries.[18] These rules must be pre-approved by relevant DP authorities of the Member States where the personal data is to be exported.

Secondly, the EU-US Safe Harbor Agreement was adopted by the Commission through Decision 520/2000/EC.[19] The Safe Harbor agreement was open to all US companies that were subject to the jurisdiction of the Federal Trade Commission (FTC) or the Department of Transportation (DOT).[20] To be eligible for the Safe Harbor, US companies must either join a self-regulatory privacy programme consisting of a set of data privacy rules with regard to data processing adhering to the Safe Harbor principle, or join an organisation running the Safe Harbor seal programme, such as TRUSTe (currently known as "TrustArc").[21] However, this Agreement was ruled to be invalid by the CJEU in 2015 because the US laws did not provide an adequate level of DP, as required by the EU DP law.[22]

1.2 EU Data Protection Law Reform

Due to the rapid development and globalisation of technology, along with the lack of consistency in DP regimes across all Member States, the Commission started the process of revising the EU DP legal framework in May 2009, with a view to (1) enhancing the internal market dimension of DP; (2) increasing the effectiveness of the fundamental rights to DP; and (3) establishing the consistency of the EU DP rules, including those in the field of police cooperation and judicial cooperation in criminal matters.[23]

On 25 January 2012, the Commission published a proposal for a comprehensive reform of the EU legal framework on DP, composed of two legislative instruments; namely

---

[18] A29WP, 'Working Document: Transfers of Personal Data to Third Countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers' 11639/02/EN WP 74, Adopted 3 June 2003.
[19] Commission, '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' Brussels, 20102004 SEC (2004) 1323.
[20] ibid; Art 1(2)(b).
[21] See <https://www.trustarc.com> accessed 1 March 2018.
[22] See more details in section 2.3.2.4.
[23] Commission Conference, 'Personal Data – More Use, More Protection?', Brussels 19-20 May 2009.

(1) the General Data Protection Regulation (GDPR), which was meant to replace the DPD;

(2) the Police and Criminal Justice Data Protection Directive (PCJDPD), which was meant to replace the Council Framework Decision 2008/977/JHA.[24] This directive aims to ensure that the data of victims, witnesses and suspects of crimes are duly protected in the context of a criminal investigation and a law enforcement action, and the more fully harmonised laws will also facilitate cross-border cooperation of police or prosecutors in attempting to combat crime and terrorism more effectively across Europe.[25]

The GDPR came into force on 24 May 2016 and became applicable on 25 May 2018.[26] Regarding the GDPR, there are a number of substantial changes that have been made to the DPD, some of which are relevant to the problems the DPD created for CSPs and cloud users. These will be thoroughly explored in the next section.

2. Analysis: What Legal Problems Affecting Trust in Cloud Computing Emerge from the Application of the EU Data Protection Law to the Processing of Personal Data in Cloud Computing

This section will discuss how the DPD which preceded the GDPR, applied to cloud computing, what problems this caused, and whether the GDPR will solve these problems. There are three problems which are about (1) the controller and the processor; (2) the territorial jurisdiction and the applicable law; and (3) the data export rules.

2.1 Who is the Controller and the Processor when Processing Personal Data in the Cloud?

The distinction between controller and processor was at first glance quite clear

[24] See more details in chapter 4, section 1.2.3.
[25] Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)' (Brussels, 25.1.2012 COM (2012) 11 final) 1.
[26] Commission, 'Legislation L119' (4 May 2016) 59 OJEU; Regulation (EU) 2016/679 of the European Parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

according to the definition provided by Article 2(d) and 2(e) of the DPD.[27] When applying these two definitions in the cloud, it might be assumed that a cloud user who place data in the cloud, is a controller who determines the purposes and the means of the processing of personal data, and a CSP who merely processes personal data on behalf of the cloud user, is a processor, as long as such CSP does not act in a manner which was inconsistent with the user' s instruction. However, different kinds of cloud service has made the distinction between the controller and the processor increasingly blurred.[28]

This situation then made it quite difficult to determine who is a controller (who is obliged to comply with almost all DP obligations imposed by the DPD) and who is a processor (who had a lesser burden, only to process personal data as instructed by the controller and to comply with the security measures for data processing) in the cloud.[29] Although some CSPs define themselves as controllers or processors in their terms of service, this was not conclusive under the EU DP law which rendered the status of the controller and the processor to different parties involved in the processing of personal data depending on what the parties actually did in the situation rather than how they labelled themselves.[30]

---

[27] Article 2(d) of the DPD defined "controller" as

> the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data...

Article 2(e) of the DPD defined "processor" as

> a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller

[28] Colette Cuijpers, Nadezhda Purtova and Eleni Kosta, 'Data Protection Reform and the Internet: the Draft Data Protection Regulation' in Andrej Savin and Jan Trzaskowski (eds), *Research Handbook on EU Internet Law* (Edward Elgar 2014) 550-551. In 2007, Kuner viewed that the multiplicity of business models made distinguishing between a controller and a processor a common problem in DP law. See Christopher Kuner, *European Data Protection Law : Corporate Compliance and Regulation* (2 edn, OUP 2007) 70-71.

[29] DPD, Arts 6, 17 and 23; The problems with regard to definitions of "controller" and "processor" regarding the DPD had been long discussed by various scholars since the mainframe computers era when the user had sole control over the processing of personal data. The main issue was that neither of these definitions fit very well some parties who are involved in the processing of personal data. See Lilian Edwards, 'Privacy and Data Protection Online : The Laws Don't Work? ' in Lilian Edwards and Charlotte Waelde (eds), *Law and the Internet* (3rd edn, Hart Publishing 2009); A29WP, *Opinion 1/2010 on The Concepts of "Controller" and "Processor"* (00264/10/EN WP 169, Adopted 16 February 2010).

[30] A29WP, *Opinion 1/2010 on The Concepts of "Controller" and "Processor"* (n29) 8; For example, Google identifies itself as merely a data processor. See Google Cloud Platform Terms of Service, section 1.4 Data Location < https://cloud.google.com/terms/ > accessed 12 April 2018.

As was explained in chapter 1 (section 4), cloud computing can be classified into two main models, i.e. the deployment model and the service model. This section provides an analysis of who is the controller and the processor under the DPD in different situations in the cloud.

2.1.1 Who is the Data Controller and the Data Processor in Cloud Services as Categorised by the Service Model?

2.1.1.1 Software as a Service (SaaS)

Cloud users may not always be sole controllers when adopting SaaS for two main reasons.

Firstly, SaaS users might not determine some of the purposes of the processing of personal data in the SaaS. For example, when Gmail processes personal data of several users, it is obvious that Gmail users will determine the purpose of the processing i.e. to send and receive email. But, at the same time, Gmail might be data mining in order to create a targeted advertisement for its own purposes. And this purpose is determined by Gmail, rather than by Gmail users.

Secondly, although SaaS users probably determine the purposes of the processing of their personal data in the SaaS, whether such users determine the means for such processing is less clear. For example, Gmail users only adopt the application that is running on the cloud infrastructure, through the Internet as a Web-based service with a limited administrative application setting. Therefore, users normally have no idea about the means that the SaaSP is using for processing their personal data, such as an application code, a server location, a security measure or an outsourcing chain. Therefore, SaaS users probably do not determine all the means of the processing of their personal data held in SaaS.

On the one hand, SaaSPs might not always be processors, who merely process personal data on behalf of the controller, due to the fact that SaaSPs have a lot of control over the underlying infrastructure of the *SaaS*, such as servers, operating system, network and security provisions. SaaSPs might determine some of the purposes of – and will be likely to determine all of the means for - the processing of personal data in the context of SaaS. All SaaSPs look quite a lot like controllers in relation to such data

processing.

SaaS users seem not to have sole control over the processing of personal data since they do not determine some of the purposes and a lot of the time they do not determine the means of the processing of their personal data. The SaaSPs seems to have a capacity to determine some of the purposes and almost all the means of the data processing. SaaSPs probably have more control over the personal data processing in the SaaS than SaaS users.

2.1.1.2 Platform as a Service (PaaS)

The PaaS offers users more control and flexibility than the SaaS. PaaS users have a full control over applications and application hosting environment configurations of the platform. For example, Google App Engine users determine how to develop and deploy an application within that platform, or another instance of it, such as application codes or security measures, but they are restricted to coding applications using only programming languages, application programming interfaces (API) and so on which are determined by Google App Engine.[31] Google App Engine as a PaaSP still takes responsibility for managing and controlling the low level of the underlying infrastructure, such as servers, operating systems, networks and virtualisation and it also takes responsibility for security provisions for such infrastructure.

PaaSPs and PaaS users seem to have joint control over the processing of personal data in the PaaS. This is because both of them have the ability to control and manage such personal data processing by determining some of the purposes and some of the means for the processing of personal data.

2.1.1.3 Infrastructure as a Service (IaaS)

IaaS users are allowed to access to raw computing resources of cloud services. Amazon EC2 users have an ability to determine and provision all aspects of deployment based on their needs, including applications, operating systems, networks and servers and they also mainly take responsibility for maintenance and security provisions beyond the basic infrastructure. However, Amazon EC2 as an IaaSP still controls the entire underlying

[31] See <https://cloud.google.com/appengine/> accessed 1 April 2018.

cloud physical infrastructure, including servers networking and virtualisation.[32]

Therefore, IaaS users are highly likely to be controllers who determine all the purposes and the means of the processing of their personal data in the IaaS. But whether IaaSPs are qualified as processors, who merely process personal data on behalf of their users, is unclear because an IaaSP is seen as a passive CSP who merely supplies equipment and infrastructure to users who themselves process their personal data.[33] Therefore, IaaSPs might not be considered to be processors since they probably do not have the ability to take any measures to affect the data processing. IaaSP users seem to have more control over the processing of personal data in IaaS than IaaSPs.

Hon et al. express their opinion that IaaSPs should not be identified as processors under two sets of circumstances which include:

(1) when IaaSPs merely host personal data, without any knowledge as to whether it is personal data (encrypted data); or

(2) when IaaSPs merely supply the utility infrastructure for users' self-service usage, without any ability to monitor the personal data processing or even to obtain access to the data.[34]

They further conclude that whether IaaSPs will be considered as processors should not be based on the fact that the personal data is being processed using their equipment and infrastructure.[35] Regarding this idea, the IaaSP might not have either a processor or a controller status in the above two situations. Hon.et al suggests that the knowledge of the nature of the processed data and the ability to control over the data processing should be a prerequisite for rendering a processor status to the party involved in the data processing.[36] Nevertheless, this would lead to further critical questions: Should IaaSPs be obliged to comply with the DP law? If the answer is 'yes', what should be the DP obligations with which IaaSPs have to comply? These issues will be discussed in the

[32] See <https://aws.amazon.com/ec2/> accessed 11 April 2018.
[33] W Kuan Hon, Christopher Millard and Ian Walden, 'Who is Responsible for Personal Data in Clouds?' in Christopher Millard (ed), *Cloud Computing Law* (OUP 2013) 210-215.
[34] ibid.
[35] ibid.
[36] Hon, Millard and Walden (n33) 215.

following section, when considering whether the GDPR can deal with the status of IaaSPs.

However, regarding the DPD, almost all the activities performed upon personal data, without the requirement to acknowledge the nature of the data, fell under the definition of "the processing of personal data" in Article 2(b) which included

> any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage...[37]

Therefore, an IaaSP which passively keeps users' data on its infrastructure or merely allows users themselves to process their personal data on its infrastructure, regardless of whether the IaaSP knows that such data are personal data, would probably act as a processor under the DPD.

2.1.2 Who is the Data Controller and the Data Processor in Cloud Services as Categorised by the Deployment Model?

2.1.2.1 Private Cloud

When the whole infrastructure is owned by only one cloud user, it is quite straightforward to identify such a user, who has sole control over the purposes for which and the means by which all the data processing within the infrastructure takes place, as a controller. A CSP who maintains the underlying infrastructure by e.g. processing data on behalf of users, allocating computer resources, will be classified as a processor. Private cloud users probably have more ability to exercise control over the processing of personal data more than private CSPs.

2.1.2.2 Public Cloud

The public cloud provides on-demand self-services over the Internet to the general public using the same infrastructure. The infrastructure is owned by third parties or public CSPs and controlled by public CSPs, but it is designed to be used by users with limited configuration, security and privacy. For instance, Microsoft Office 365 as a public CSP provides users with access to office applications plus other productivity

[37] DPD, Art 2(b).

services, such as online storage services through the Internet, and it takes the responsibility of managing the whole infrastructure and pooling resources into the capacity required by its users.[38]

Whether public cloud users will be controllers is less clear, since they seem to find it difficult to exercise any meaningful control over their data processing and the way in which public CSPs operate. Users might not be able to determine some of the purposes and do not seem to determine all the means of the data processing in the public cloud. On the other hand, public CSPs, who are in charge of almost all the installation, provision and maintenance of the infrastructure, probably do not only process personal data on behalf of users, but also determine some of the purposes and almost all the means of such data processing. Public CSPs probably have much more ability to control and operate the data processing than public cloud users.

2.1.2.3 Community Cloud

The community cloud sits between private and public clouds. The infrastructure is somewhat similar to the private cloud, but is operated exclusively for a specific community of users who have common interests, privacy, security and regulatory considerations. This service utilises spare capacity of the IT infrastructure within several organisations (as users) by enabling a cloud infrastructure where all resources are virtualised and used on a shared basis. This infrastructure could be internally managed by users or by a third party.

For example, community cloud provided by Salesforce is built on the Salesforce platform, but the security architecture of the platform is used by organisations around the world. It allows users to control and manage services through administrative permissions to the data access and sharing model.[39]

Community cloud users might not be controllers since the application on and the environment in the whole infrastructure in which several hosting organisations (as users) allow other cloud users to obtain access, will be determined and operated by such

[38] See <https://products.office.com/en-gb/business/microsoft-office-365-frequently-asked-questions> accessed 1 April 2018.
[39] See <http://www.salesforce.com/communities/faq/> accessed 1 April 2018.

hosting organisations. Therefore, cloud users do not seem to determine some of the purposes and the means of the processing of personal data in the community cloud. The community CSPs, who control the virtualisation of the whole cloud infrastructure, might determine some of the purposes and the means of the processing of personal data, so that this provider might not be merely a processor, but sometimes might have the possibility of being able to control and manage the processing of personal data in the community cloud. Both community cloud users and community CSPs have a joint control over the personal data processing in the community cloud.

2.1.2.4 Hybrid Cloud

The hybrid cloud is more complex than other deployment model. It is an integrated cloud service utilising private, public and community clouds to perform distinct functions within the same organisation, but at the same time they are bound together by standardised or proprietary technology that enables data and application portability. In the hybrid cloud, users can deploy an on-premises private cloud to host confidential data, but use a third-party public CSP to host less-critical resources. For example, Skytap Hybrid Cloud offers users with self-service network configuration that users can connect their private clouds to the public cloud in order to create the hybrid cloud. When the private and the public cloud work together via a VPN connection, users can bring up new virtual machines and applications from a shared template/catalog set out by Skytap.[40] Since the hybrid cloud involves the composition of two or more types of cloud services, an ability to take control over the data processing of the hybrid cloud is based on which cloud deployment model of cloud services is being used to process personal data. Hybrid cloud users do not seem to have sole control over the data processing. Hybrid CSPs can also determine the means of such data processing, so that these CSPs might be considered to be controllers.

2.1.3 Who is the Data Controller and the Data Processor in Case of Multi-Layer Cloud Services

Due to the fact that one kind of cloud service could be layered on top of another kind of cloud service, there might be more than one party involved in the same personal data

[40] See < https://www.skytap.com/blog/how-to-build-a-hybrid-cloud/ > accessed 1 April 2018.

processing. The more sub-CSPs get involved, the more complex it is to try to identify a controller and a processor in the cloud.[41] And since one CSP can play different roles in relation to the same set of personal data processing, he could be either the controller, the processor or neither of these of such data processing.

According to figure 3, company A (an SaaSP) provides a mail service to Mr. David by building on a platform of company B (a PaaS) and, at the same time, company B builds its service on an infrastructure of company C (an IaaS). Mr. David, who probably determines the purposes and the means of the data processing, is likely to acts as a controller and company A, which processes the data on behalf of Mr. David, is likely to act as a processor.

Then, when company A subcontracts company B to deliver its service to Mr. David, company B (a sub-CSP) seems to be a sub-processor which processes Mr. David's data on behalf of Mr. David. However, if company A or company B process Mr. David's data for their own purposes e.g. advertisement, such a provider probably acts as a controller, rather than a processor of such data processing. Thus, in this case, company A and company B could be either the controller or the processor of the different processing of the same personal data of Mr. David.

[41] Paul M. Schwartz, 'Information Privacy in the Cloud ' (2013) 161 U Pa L Rev 1623, 1626.

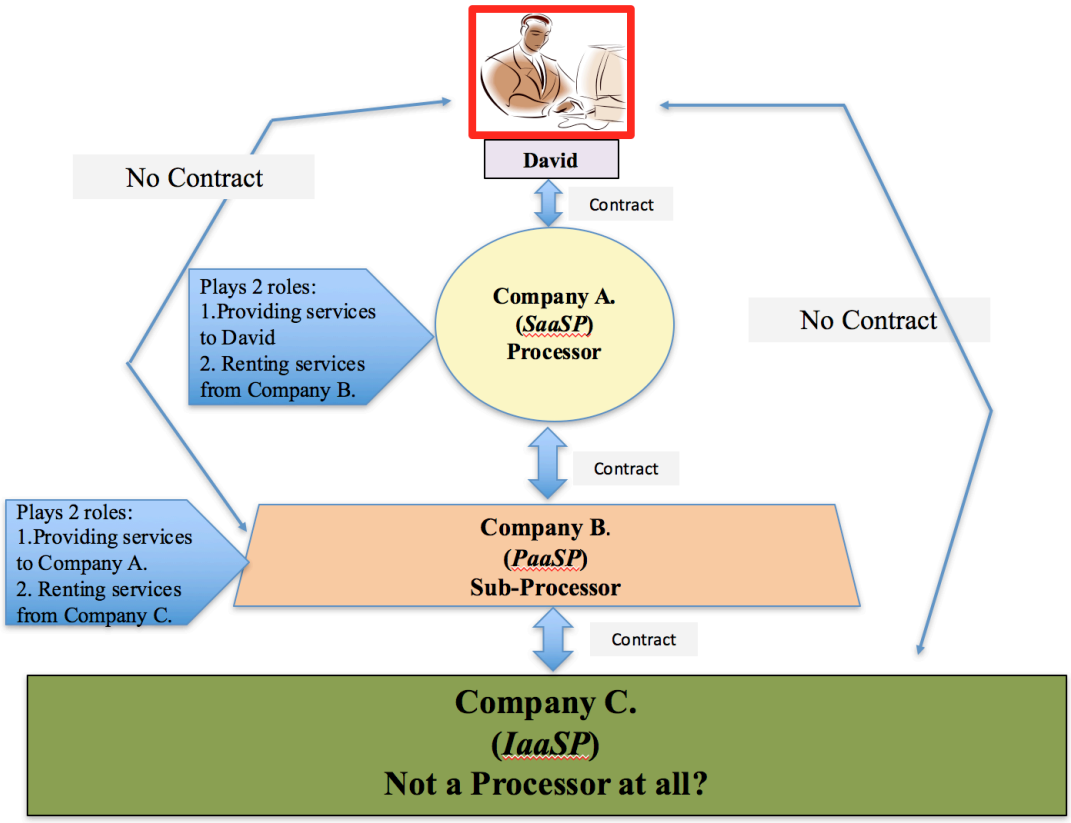

Figure 3. An Example of When the Same CSPs Play Different Roles in the Same Data Processing

Furthermore, there is a problem with identifying the status of each of sub-CSPs due to the fact that several sub-CSPs play different roles when they get involved in the processing of personal data. The question remains whether all sub-CSPs will be qualified as sub-processors?

According to figure 3, company B and company C are the sub-contractors (sub-CSPs) of company A. While company B, which is a PaaSP, can process personal data of Mr. David, company C, which is an IaaSP, merely provides processing equipment, hosting infrastructure and technical support for the use of company B (as a sub-processor of the processing of personal data of Mr. David) to provide services to company A and it has no ability to control or process personal data of Mr. David. Accordingly, company B is probably a sub-processor, but company C is unlikely to be a

sub-sub processor, who is obliged to comply with security obligations regarding to the DPD, of the processing of personal data of Mr. David, (or even as a controller). This would lead to the question: whether company C is liable towards Mr. David for damage resulting from data breach caused by company C.

Apart from that, the sub-contracting arrangement could possibly further complicate matters in ways which are likely to produce risks to cloud users.[42] When a CSP to whom cloud users entrust their data subcontracts with other CSPs to deliver services to its users, CSPs do not often present their users with information about an outsourcing chain, which might consist of multiple sub-CSPs.[43] Consequently, it is quite difficult for cloud users to find out who is involved in their data processing behind the CSPs with whom they are in contract. And since users do not have the ability to choose the sub-CSPs by making their own decisions, they are not in a position to assess the risks that are involved in their data processing.

Even if the information about all sub-CSPs in the outsourcing chain is available to cloud users, sub-CSPs are unlikely to deal with requests of individual users. The lack of any direct contractual relationship between sub-CSPs and users will make it difficult to enforce obligations placed on sub-CSPs towards users. In principle, users could not hold sub-CSPs liable even in the case of the breach and misuse of personal data caused by such providers unless those obligations are enforced by processors who have contracts with sub-processors and have inserted suitable obligations.

An example can be seen in Figure 3, where Mr. David has no direct contractual relationship with companies C and B. Therefore, he is unable to make a direct request to either of these companies, which probably don't even know about the relationship between Mr. David and company A. Even in the event of a data breach caused by company C or B, Mr. David could not hold them contractually liable for such damage. However, company A, with whom Mr. David has a contract, still have to be liable for such a data breach as stated in the contract. Company A is likely however to ask for

[42] Henry Chang, 'Data Protection Regulation and Cloud Computing' in Anne S.Y. Cheung and Rolf H. Weber (eds), *Privay and Legal Issues in the Cloud* (Edward Elgar Publishing Limited 2015) 38-40; Hon, Millard and Walden 'Who is Responsible for Personal Data in the Clouds'(n33) 203-204.
[43] A29WP, *Opinion 05/2012 on Cloud Computing* (01037/12/EN WP196, Adopted 1 July 2012) 2.

indemnities or duties of care from company B and perhaps even company C depending on the contractual links.

The analysis in the previous sections shows that cloud users might not always be the sole controller and CSPs might not always be merely processors since they are sometimes also able to determine some of the purposes and some of the means for the data processing in the cloud. The concept of joint controllership, which was recognised by Article 2 (d) may address the status of only some kinds of CSPs who have a possibility to jointly determine the purpose or the means of the data processing.[44] But there is still a problem with regard to DP obligations among joint controllers since the DPD did not provide any information about their obligations, which reflect their actual roles and their relationships with cloud users.

2.1.4 Does the GDPR Improve the Situation?

2.1.4.1 Categorisation

The definition of controller and processor in Article 4(7) and (8) of the GDPR remain the same as in the DPD, even though the Commission has acknowledged the difficulties involved in applying such provisions in the cloud.[45] Article 26(1) of the GDPR however does formally recognise that CSPs may be "***joint controllers"*** and provides its description as

> where two or more controllers jointly determine the purposes and means of processing, they shall be *joint controllers*.

The joint controller is not a completely new concept (see previously at page 73).[46] But the GDPR promotes the position of joint controller more heavily as a separate actor by providing its definition and imposing specific obligations on this actor to determine its respective responsibilities for compliance with the GDPR by means of an arrangement

[44] Cloud C, *Overview Report of Legal and Regulatory Requirements in Data Management* (Coco Cloud: Confidential and Compliant Clouds, D21, 30 April 2014) 15.
[45] Neelie Kroes, *EU Data Protection Reform and Cloud Computing* (Data Protection Reform and Cloud Computing "Fuelling the European Economy" Event, Brussels, 30 January 2012 SPEECH/12/40)
[46] DPD, Art 2(d).

between them.[47]

Indeed, the concept of a joint controller perpetuates the binary assumptions in the DPD that there are only controllers or processors in the data processing, so that the joint controller does not respond to the different levels of the actual control over the data processing in the cloud by different kinds of CSPs.[48] Considering the SaaSPs, PaaSPs, public CSPs, community CSPs and hybrid CSPs who have different level of control over the processing of personal data as joint controllers probably does not help to improve the existing situation.

The arrangement determining the respective duties between joint controllers to comply with the GDPR, would help clarify responsibilities among joint controllers as regards their internal relationships and their relationship to the data subject. This could deal with the question of who will be liable in the event of any breach or misuse of personal data when a range of controllers are involved in the same processing of personal data. This provision would also have critical implications for any outsourcing arrangement because a range of companies, which is likely to act as a joint controller, will need to modify their commercial arrangements in order to fulfill the obligations with regard to Article 26.[49]

However, this position is likely to pose further problems about the respective obligations of the controller and the processor. For example, if the SaaSPs, PaaSPs, public CSPs, community CSPs and hybrid CSPs are qualified as joint controllers, there would not be a processor for such data processing. The question arises who will be responsible for complying with DP obligations that the GDPR specifically imposes upon the processor (see section 2.1.4.2) in order to protect the DP right of the data subject.

2.1.4.2 Obligations

In term of controller' s obligations, the GDPR continues to keep general DP obligations for ensuring that the processing of personal data is compliant with the EU DP law and

[47] GDPR, Art 26(1).
[48] Mark Webber, 'The GDPR's Impact on the Cloud Service Provider as a Processor' (2016) 16 PDP J 11, 14; Cuijpers, Purtova and Kosta (n28) 515.
[49] Christopher Kuner, *The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law* (Privacy and Security Law Report 11 PVLR 06, 02/06/2012) 13.

imposes a range of new obligations which include the requirement:

(1) to be able to demonstrate that the data processing is performed in compliance with the GDPR. The GDPR also provides guidelines on how the controller can demonstrate compliance, e.g. to adopt internal policies or to adhere the processor to an approved code of conduct;[50]

(2) to comply with the principles of DP by design and default by implementing appropriate technical and organisational measures, ensuring that data is only processed where and for as long as necessary and generally complying with the requirements of the GDPR;[51]

(3) to maintain a record of all categories of the processing activities that take place under its responsibility, e.g. the names and contact details of controllers;[52]

(4) to cooperate on request with the DPAs in the performance of its tasks;[53]

(5) to notify of any personal data breach to the competent DPA, not later than 72 hours after having become aware of it;[54]

(6) to communicate a personal data breach to the data subject without undue delay, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;[55]

(7) to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data;[56]

(8) to designate a DP officer in certain circumstances, such as when the processing is carried out by a public authority or body, except for courts acting in their judicial capacity.[57]

In term of processor' s obligations, some of the new processor's obligations are similar to those of the controller, e.g. to maintain all the categories of the processing

[50] GDPR, Art 24 and Recs 78, 81.
[51] GDPR, Art 25.
[52] GDPR, Art 30.
[53] GDPR, Art 31
[54] GDPR, Art 33.
[55] GDPR, Art 34.
[56] GDPR, Art 35.
[57] GDPR, Art 37.

activities under its responsibility, to notify of any personal data breach to the competent DPA.[58] The processor is also obliged to be liable for non-compliance with the GDPR.[59]

In addition, the GDPR specifically set out the extra obligations for the processor in Article 28 which include

(1) to get the specific or general written authorisation of a controller before engaging with another processor;[60]

(2) the requirement that the processing by the processor should be governed by a written contract or legal act, including in electronic form, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing and the type of personal data and categories of the data subject and obligations and rights of the controller. And that contract or legal act shall stipulate the processor[61]

(a) to process the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation;[62]

(b) to implement appropriate technical or organisational measures as possible in order to assist the controller for the fulfillment of the controller's obligation to respond the data subject' rights;[63]

(c) at the controller's choice, to either return or destroy the personal data at the end of the relationship except as required by EU or Member State law;[64]

(d) to provide the controller with all the information necessary to demonstrate compliance with the GDPR and allow for audits, including inspections conducted by the controller or another auditor mandated by the controller.[65]

The GDPR focuses heavily on strengthening the responsibilities of both the controller and the processor by imposing more stringent and extensive obligations on

[58] GDPR, Art 30, 31, 33 and 37.
[59] GDPR, Art 82.
[60] GDPR, Art 28(2)(4).
[61] GDPR, Art 28(3) and 28(9).
[62] GDPR, Art 28(3)(a).
[63] GDPR, Art 28(3)(e).
[64] GDPR, Art 28(3)(g).
[65] GDPR, Art 28(3)(h).

both of them. It places more statutory DP obligations on the processor because the Commission has realised that in fact the processor is also doing quite a lot of the controlling in the processing of personal data. Accordingly, when CSPs act as processors, they will have to comply with a range of obligations to preserve the security of the data that have been processed in the cloud. Nevertheless, some of the new obligations set forth in Article 28 are considered not quite to suit the service model of cloud computing.[66]

First, it makes no sense for the processors to get prior authorisation from all the controllers to whom they provide services and with whom they have a contract every time they engage with sub-processors.[67] This is because there might be a multiplicity of possible architectures for what appears to end users by using, e.g. SaaS built on IaaS or SaaS built on PaaS which is built on IaaS. In such architectures, some sub-processors (typically IaaSPs) may not have a direct contractual relationship with the controller (they might not even know whether there is a relationship between the processor with whom they have a contract and the controller).

One way to deal with the problem will be by processors requiring sub-processors in the relevant contract to incorporate terms requiring the getting of prior authorisation from the original controller. This is likely to lead to a network of complex and difficult to perform and enforce contracts. This would not be helpful for CSPs as processors, who normally want to reserve flexibility over their operation, to provide economic cloud services, especially CSPs serving thousands of users.[68]

Furthermore, controllers are unlikely to have an interest in giving such an authorisation since their expertise will not be, e.g. in IaaS. They placed their faith in the lead processor selected based on factors such as price and reputation. CSPs will find this duty burdensome in the extreme. They will have already selected their infrastructure suppliers to serve their whole business before making their services available to the controller. It is not reasonable or possible for CSPs to re-engineer their entire

[66] In this analysis, a cloud user is assumed to be a controller and a CSP is assumed to be a processor.
[67] GDPR, Art 28(2)(4); Hon WK, 'Killing Cloud Quickly, with GDPR' (4 February 2016) <http://www.scl.org/site.aspx?i=ed46375> accessed 1 November 2016.
[68] Webber (n48) 13.

infrastructure based on the instructions of each controller. The choice is really for a controller either to stop using cloud computing entirely or to go to different processor. The obligation is thus burdensome for all without conferring benefit.

Second, the obligation of the processors to process personal data only on "documented" instructions from the controller seems to be impractical for the processors. There are some problems regarding the meaning of "documented" instructions. Do they mean "written" instructions? Do they include the documents in electronic form, such as when the controllers click on a button from their browsers?

Moreover, whether this obligation also applies to sub-processors or sub-sub processors, who process the same set of personal data, is unclear. If the answer is "yes", then it will be even more difficult for such processors to comply with this obligation since they do not have a direct contractual relationship with the controller.[69]

Hon. also argues that this obligation does not make any sense in the cloud where CSPs do not actively process personal data as the users instruct, but where users access cloud services directly themselves, in a self-service fashion.[70] Arguably, as was discussed in section 2.1, the controller does not always have the sole control over the data processing by determining all the purposes and the means of the data processing in the cloud, but the controller has to be in some way instructed, (e.g. by means of data processing for SaaS users). Therefore, processing personal data purely according to the instructions of the controller is probably impossible in the cloud.

2.1.5 Beyond the GDPR

2.1.5.1 A New Category of Actor

Staiger is of the view that the simple definitions of the controller and the processor under the GDPR pose challenges in identifying the controller and the processor in the cloud. He agreed with Hon. et al. that CSPs who will be qualified as processors should be required to have knowledge of the personal data processing on their infrastructure and to

[69] See the situation when there are more than one sub-processors involved in the same set of the personal data processing as discussed in section 2.1.3

[70] W Kuan Hon, 'Killing Cloud Quickly, with GDPR' (4 Febuary 2016) <http://www.scl.org/site.aspx?i=ed46375> accessed 1 November 2016.

have control over the data in the form of access to the data.[71] Finally, he suggests that a new category should be imposed in dealing with CSPs who are neither controllers nor processors under the DPD and the GDPR.[72]

Staiger's approach would be more helpful if he supplied further details about the new category, e.g. the concept, the definition and the DP obligations that would apply to this new actor. However, since the GDPR has not yet provided the details about the new actor, this might lead to many questions, e.g. Do we really need the new category of the actor? Could this new category help dealing with the problems about the status of a range of actors who get involved in the processing of personal data in the cloud? What should be the DP obligations applying to this actor? Do we need to modify the current concept of the controller and the processor and their DP obligations with a view to making them to be consistent with the concept of this new actor?

2.1.5.2 A Neutral Intermediary

Hon et al. opine that there are some difficulties in distinguishing the roles of the controllers and the processors in the cloud because the definitions of the processor and the controller under the GDPR do not reflect the realities of cloud services.[73] They suggest, as we have seen, that it is too burdensome to classify an IaaSP as a processor, and that a new categorisation as a neutral intermediary, e.g. a phrase associated with the E-Commerce Directive 2000, might be helpful.[74]

According to the E-Commerce Directive 2000 (ECD), intermediary service providers who provide Information Society Services (ISS), which the ECD has defined as 'any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing, and at the individual request of a recipient of the service'

---

[71] See section 2.1.3; Hon, Millard and Walden 'Who is Responsible for Personal Data in the Clouds'(n33) 210-215.
[72] Dominic N. Staiger, 'Cross-Border Data Flow in the Cloud Between the EU and the US' in Rolf H. Weber and Anne S.Y. Cheung (eds), *Privacy and Legal Issues in Cloud Computing* (Edward Elgar Publishing 2015) 103.
[73] W Kuan Hon and others, *Cloud Accountability: The Likely Impact of the Proposed EU Data Protection Regulation* (Tilburg Law School Legal Studies Research Paper Series, No 07/2014) 19.
[74] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market.

have the benefit, under certain conditions, of the immunities in Articles 12-15.[75] Recital 18 of the ECD however states that a free service provider does not fall outside the scope of the ECD, if the service represents part of an 'economic activity'.[76] Accordingly, CSPs, including those who provide free services (for example in the case of Google who provide free cloud services e.g. Google Drive, Gmail, but make money from associated advertising) seem to be able to rely on such immunity.

The ECD provides an immunity from legal liability for Information Society Services Provider (ISSPs) who act as host providers (who host or store more than transiently content produced by third party) providing that such providers are not liable, as long as

(1) for criminal liability: the providers do not have any actual knowledge of the illegal nature of the activity or information; for civil liability: the providers are not aware of any facts or circumstances from which the illegal activity or information would be apparent and;

(2) the providers, upon obtaining such knowledge or awareness, act expeditiously to remove or disable access to the information.[77]

Applying this concept in the cloud, the knowledge and the ability to exert control over personal data would be a pre-requisite for any liability of CSPs. Hon et al. further recommend the need to modernise the ECD, which currently excludes matters of DP law from its scope, to include this DP matter or to introduce a similar defense for processors in relation to DP law, and then to introduce liability defences for mere intermediaries which will apply to DP law matters.[78]

The notion of a neutral intermediary under the ECD is quite interesting, but fits badly into the general scheme of the GDPR. A requirement to have actual or constructive knowledge (in Article 14, ECD) about the nature of the data and any

[75] ECD, Art 2(a).
[76] ECD, Rec 18. See Lilian Edwards, 'The Fall and Rise of Intermediary Liability Online' in Lilian Edwards and Charlotte Waelde (eds), *Law and the Internet* (Hart Publishing 2009) 63; C484/14 *Mc Fadden v Sony Music Entertainment Germany GmbH* [2016] CJEU, judgment of 16 March 2016. This may still exclude public sector services which are not designed to make money, e.g. e-government cloud services.
[77] ECD, Art 14.
[78] ECD, Art 1(5)(b).

illegality in how it is processed before liability followed might be a helpful concept for processors and sub-processors. However, modernising the ECD to include these DP matters might not work and is currently not on the table. Indeed the GDPR, like the DPD before it, specifically says that nothing in it is to affect the ECD and the two instruments have generally had no interrelationship.[79]

2.1.5.3 All Data Controllers, No Data Processors

De Hart and Papakonstantinou suggest that the preferable way to deal with all these problems is 'to boldly abolish the notion of data processor and vest the controller the title, rights and obligations upon anyone processing personal data, regardless of its means, purposes'.[80]

This concept does seem to be impractical in the cloud. The absence of the position of a processor is likely to bring about a number of problems regarding the status and DP obligations of several actors get involved in the processing of personal data in the cloud. If all processors were controllers, they would directly owe very heavy obligations towards all data subjects whose data they processed. For those who are traditionally qualified as sub-processors, they would also have a very heavy burden to comply with DP obligations under the EU DP law. The contractual obligation (between the controller and such sub-processors) would not be necessary. This situation would give rise to problems of enforcing it globally.

2.1.6 Conclusions

The DPD set out a rule for identifying the parties who was involved in the processing of personal data, which was based on the model of a binary division between those who controlled the means and purposes of processing, and those who merely implemented those instructions. This binary model derived from the 1970s and 80s when data warehousing was common and data processing was often performed not by the actor who wanted the processing done, but by an agent, in response to the instructions given by each users. Sub-processors were rare and the whole business could be defined easily

[79] GDPR, Rec 21.
[80] Paul De Hert and Vagelis Papakonstantinou, 'The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System fo the Protection of Individuals' (2012) 28 CLS Rev 130, 133.

in a written contract.

Due to technological development, the business environment has changed completely. With cloud computing, the user as the controller may technically be in charge, but sometimes the CSPs (who traditionally are categorised as processors) will have the ability to take control of the means of processing, if not the final purpose. Some CSPs have more control than others. Some are aware of the user as a controller, others are only aware of the processor who employed them. The situation in the cloud does not fit the binary model described above which the law has used since the DPD.

The Commission has attempted to address this problem by promoting the existing idea of joint controller in the GDPR and by placing greater obligations on processors. However, this will likely simply create more problems, especially now that cloud computing is typically implemented in a nested and automated way. As noted above, the division of control of the purposes and means of processing is no longer a binary division between controller and processor. Instead, it seems more like a sliding scale. Accordingly, a model that would assess the qualitative level of the control exercised by a particular CSP and allocated either liability or immunity accordingly, might be a useful starting place to consider.

2.2 When does the EU Data Protection Law Apply to the Processing of Personal Data Held in the Cloud and Which Member State Laws Apply to the Processing?

There were two main objectives of Article 4, as stated in the travaux préparatoires and the preamble to the DPD:

(1) to avoid a situation in which data subjects find themselves outside the protection of the EU DP law;

(2) to avoid a situation in which the same data-processing operation is governed by the laws of more than one country.[81]

In order to strike a balance between these two objectives, Article 4 set out two

[81] Commission of the European Communities, *Amended Proposal for Council Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data* (Com(92) 422 final - SYN 287, Brussels, 15 October 1992).

main rules for the applicability of the DPD for two different purposes.[82]

The first rule determined when the EU DP law applied to the processing of personal data (a question of territorial scope). CSPs were subject to EU DP law under circumstances where

(1) CSPs were established in the EU ("EU CSPs") and the processing was carried out in the context of the activities of such an establishment;[83]

(2) CSPs were not established in the EU ("non-EU CSPs"), but

(a) the establishment of such CSPs was located in a place where the EU law applies by virtue of international public law, such as in the case of data processing by embassies in a foreign country or on a ship (e.g. a floating data centre, in which Google has a patent);[84]

(b) When such CSPs were using "equipment" in the EU to process personal data.[85]

The second rule identified which Member State laws applied to the processing of personal data (a question of choice of applicable law). Once CSPs fell under the territorial scope of the DPD, they had to comply with the DP law of the Member State where

(1) the establishment of EU CSPs was located. If such CSPs had more than one establishment (e.g. offices/branches located in multiple Member States), the DP law of the Member State where the establishment in which the data processing taking place in the context of the activities of such an establishment was located will apply to such data processing. However, CSPs were still obliged to ensure that each of their establishments complies with the local requirements of the DP law of the Member States where each of

[82] DPD, Art 4.
[83] DPD, Art 4(1)(a).
[84] DPD, Art 4(1)(b) and Rec 18. See <http://www.google.co.uk/patents/US7525207> accessed 1 January 2018. The criteria from public international law will determine in specific situations the law applicable to the data processing beyond the national boundaries. For example, the data processing by embassies will be subject to their national DP law. See A29WP, *Opinion 8/2010 on Applicable Law* (0836-02/10/EN WP 179, Adopted 16 December 2010) 18; Martin Dixon, *Textbook on International Law* (7 edn, OUP 2013) chapter 6 ; Malcolm N. Shaw, *International Law* (7 edn, CUP 2014) chapter 10.
[85] DPD, Art 4(1)(c).

the offices was established;[86]

(2) the equipment used by non-EU CSPs for processing personal data was situated.[87] Article 4(2) required these non-EU CSPs to appoint a representative in that State.

In practice, applying these two rules in the cloud faces a number of problems as follows:

2.2.1 Problems in the Case of the EU CSPs Regarding Article 4(1)(a) of the DPD

2.2.1.1 "Establishments"

It is not always easy to identify whether each of CSPs has their establishment in the EU. This is because many of the popular CSPs have their main establishments in the US, e.g. Google and Facebook. The question arises whether their offices/branches, which are located in the EU are qualified to count as an "establishment" under the DPD, which then means that such CSPs are subject to the EU DP law.

The DPD did not provide a definition of an "establishment". Some scholars, e.g. Bygrave, have thus argued that the legal parameters of the concept of an "establishment" are quite opaque and these would lead to difficulties in applying them online.[88] However, the preamble of the DPD did note that

> an establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements; whereas the legal form of such an establishment, whether simply branch or a subsidiary with a legal personality, is not the determining factor in this respect….[89]

Considering the jurisprudence of the CJEU concerning the freedom of an establishment under Article 50 of the TFEU as constituting a guideline, in 1985 the CJEU indicated in

[86] DPD, Art 4(1)(a).
[87] DPD, Art 4(1)(c).
[88] Lee Bygrave, 'Determining Applicable Law Pursuant to European Data Protection Legislation' (2000) 16 CLSR 252, 255.
[89] DPD, Rec 19.

Bergholz that a stable establishment required that 'both the human and technical resources necessary for the provision of particular services are permanently present'.[90] Then, in *Lease Plan Luxembourg*, the CJEU pointed out in 1988 that an "establishment" should 'possesses a sufficient degree of permanence and a structure adequate, in terms of human and technical resources, to supply the services in question on an independent basis'.[91] In the *Weltimmo,* the CJEU held in 2015 that the fact that 'the representative acts with a sufficient degree of stability through the presence of the necessary equipment for provision of specific services concerned in the Member State in question' was sufficient to constitute a stable establishment.[92]

Regarding the above cases, the "establishment" qualified under Article 4(1)(a) is probably composed of two elements;

(1) a stable technical facility or instrument for the processing of data;

(2) a sufficient degree of real activities performed by humans through such an establishment.

A branch or an office of CSPs which is located in the EU clearly thus qualifies as an "establishment" under Article 4(1)(a) of the DPD. But the mere presence of technical instruments for the processing of data, such as servers, or computers for processing personal data, is unlikely to constitute such an "establishment".[93] The German Court in the *Facebook Ireland* held in 2013 that content delivery networks for data processing were not "establishments".[94]

2.2.1.2 "In the Context of the Activities of an Establishment"

The secondary test come into play as a wider test implies that jurisdiction can be found "in the context of the activities of an establishment" rather than simply by examining the establishment alone. This test can also be used to identify which Member State law

[90] CJEU judgment of 4 July 1985, Bergholz, (Case 168/84, ECR [1985] p. 2251, para 18).
[91] CJEU judgment of 7 May 1998, Lease Plan Luxembourg / Belgische Staat (C-390/96, ECR [1998] p. I-2553, para 24).
[92] Case C-230/14 Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság ([2015] No. 111/15, CJEU, Judgment of 1 October 2015, para 30.
[93] The CJEU's Google Spain judgment in 2014 has had a considerable impact on the territorial scope of Art 4(1)(a) of the DPD. See (n100).
[94] Facebook Inc. and Facebook Ireland Ltd. v. ULD, 8 B 60/12 and 8 B 61/12 Judgment of 14 February 2013.

applies to the data processing.

Applying this test in the cloud faces many challenges because a CSP often has more than one establishment located in different EU countries. For example, Google has regional business and sales headquarters, including ones in Dublin, with a range of local offices in the EU Member States.[95] The question arises in which establishment the data processing is taking place "in the context of the activities of this establishment" (jurisdiction) and which one triggers the applicability of the Member State law to the processing of personal data (application law).

The A29WP examined these problems in 2010 and recommended three factors that should be taken into account:

(1) the degree of involvement of the establishment in activities in the context of which personal data are processed;

(2) the nature of activities of the establishments (whether or not activities are involved in the data processing);

(3) the objective of the DPD in guaranteeing effective DP.[96]

Furthermore, it should consider what is the true role of each an establishment, and which activity is taking place in the context of which establishment.[97] The applicable law will be the law of the Member State where an establishment is processing personal data in the context of its own activities.

However, CSPs might have more than one relevant establishment performing activities as *core functions* relating to the same data processing in the context of their own establishments for providing services to their users.[98] The possibility is also envisaged by Article 2(d) of the DPD that a controller is a body 'which alone or jointly with others determines the purposes and means of the processing of personal data...'. Therefore, such CSPs are likely to be subject to multiple and potentially conflicting DP laws of different Member States. This issue has been dealt with by the court in a number

[95] Google's Location <https://www.google.com/about/careers/locations/> accessed 11 March 2018.
[96] A29WP, *Opinion 8/2010 on Applicable Law* (n84) 11-12.
[97] Ibid 15.
[98] W Kuan Hon, Julia Hornle and Christopher Millard, 'Which Law(s) Apply to Personal Data in Cloud ?' in Christopher Millard (ed), *Cloud Computing Law* (OUP 2013) 225.

of cases, as will be discussed as follows.

In *Facebook Ireland, Facebook Inc. v Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein,* the German court ruled in 2013 that the Irish DP law applies to this case, rather than the German DP law, since Facebook's Irish subsidiary was an establishment of Facebook Inc. under Article 4(1)(a) of the DPD.[99] Also it was based in Dublin, Ireland, which was the only establishment in the Facebook group that had control over the personal data of Facebook members outside North America and which had the employees and the equipment to effectively exercise control over the handling of the data. By contrast, Facebook's German subsidiary was merely responsible for marketing and no personal data of German users were ever processed in the context of the activities of this German establishment.

In 2014, the territorial scope under Article 4 of the DPD was radically expanded by *Google Spain v AEPD and Costeja Gonzalse*.[100] The CJEU held that Google Spain, as a subsidiary of Google Inc. (a non-EU company), was an establishment of Google Inc. on Spanish territory, within the meaning of Article 4(1)(a) of the DPD. Although Google Spain neither designed nor operated Google's search business in Spain (the processing of the personal data at issue was carried out by Google Inc., which was in the US, rather than Google Spain), the advertising space sale generated by Google Spain was conducted 'in the context of the activities' of the Spanish establishment in order to make Google Inc. profitable. Thus the EU DP law applied in this case.

There may be two reasons why the court reached this conclusion. First, it was found that Google Spain engaged in the effective and real exercise of activities through a stable establishment in Google Spain and thus this constituted a subsidiary of Google Inc. on Spanish territory.[101] Secondly, there was an 'inextricable link' between the advertising activities of Google Spain and Google Inc.'s search engine, as without the sales and promotion of online advertising the search engine would not be economically

[99]See (n94); Schleswig-Holstein Administrative Court of Appeals Az. 4 MB 10/13, 4 MB 11/13 Judgment of 24 April 2013.
[100] Case C–131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González [2014] CJEU, Judgment of 13 May 2014.
[101] ibid para 49; DPD, Rec 19.

profitable.[102] Accordingly, the court held that the Google local corporation office in Spain was subject to Spanish DP law.

Following that, the CJEU seemed to stick with its stance in *Google Spain*, by ruling in 2015 in *Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság* that the activities of Weltimmo, a Hungarian company, which was registered and based in Slovakia, but ran property selling websites regarding Hungarian property, were subject to the Hungarian DP law.[103] This resulted from many factors which were found to be enabling the activities of Weltimmo in Hungary which took place in the context of the activities of the Hungarian establishment under article 4(1)(a) of the DPD, including that (1) the real and effective activities of Weltimmo were pursued in Hungary; (2) it used a bank account and letter box in Hungary for its business purposes; (3) there was a permanent presence of a representative of Weltimmo in Hungary; (4) the representative in Hungary represented the company in the administrative and judicial proceedings and (5) the website was involved in selling Hungarian real estate in the Hungarian language which targeted Hungarian customers.

Then, in 2016 the CJEU's decision in *VKI v Amazon*, followed the position of *Weltimmo*.[104] The CJEU was asked by VKI, an Austrian consumer protection body, to consider whether Amazon, with its registered branch in Luxembourg, amounted to an establishment in Austria when selling goods remotely through its Amazon.de website to consumers in Austria. If Amazon's activities in Austria were considered to be carried out by an establishment under Article 4(1)(a) of the DPD, Amazon would be obliged to comply with Austrian DP law when processing personal data. But Amazon argued that the Luxembourg DP law applied, as was stated in its unilaterally imposed standard contract.

The CJEU referred to the judgment that it gave in *Weltimmo*, and reaffirmed the concept that (1) a permanent branch was not needed in order to have establishment;(2) an establishment included any 'real and effective activity, even a minimal one, exercised

[102] ibid para 56.
[103] See (n92).
[104] Case C‑191/15 Verein für Konsumenteninformation (VKI)v Amazon EU Sàrl [2016] CJEU, Judgment of 28 July 2016.

through stable arrangements';(3) the data processing did not have to be carried out specifically by the establishment, simply that is was carried out in the context of the establishment would be enough.[105] Therefore, the fact that Amazon was registered in Luxembourg, without having a branch in Austria, did not, in itself, mean that Amazon did not have an establishment in Austria and, at the same time, the fact that Amazon was selling goods to Austrian consumers through its German language website did not, in itself, mean that Amazon was established in Austria.[106] The CJEU finally held that it was for the Austrian national court to determine whether data processing was being carried out in the context of the activities of the establishments within its jurisdiction. At the time of writing, we still await that decision.

However, the decision of the Administrative Court of Hamburg in *Facebook Ireland* in 2016, did contrast with the Google Spain case by overturning the Hamburg DPA order against Facebook and holding that the Irish DP law applies to the case, irrespective of there being a Facebook office in Germany.[107] In this case, a woman complained to the Hamburg DPA after Facebook enforced its real name policy by blocking her account for using a pseudonym, requesting a copy of identification and unilaterally changing her user name to her real name. The Hamburg DPA found against Facebook and held that it was not allowed unilaterally to change users' chosen usernames to their real names, nor to demand official identification documents under the German DP law which provides the right to a pseudonymous online profile. The Hamburg court found that both Facebook Ireland and Facebook Germany constitute an establishment within the meaning of Article (4)(1)(a) of the DPD, but that the Irish DP law applied due to the fact that the Irish establishment, which is Facebook's EU headquarters, was most closely associated with the disputed data processing regarding the 'real name' policy.

The term "in the context of activities" has been interpreted in a very broad manner

[105] See (n92), para 31, 41.
[106] Opinion by Advocate General Henrik Saugmandsgaard Øe in VKI, Court of Justice of the European Union, C-191/15, June 2, 2016, para 129.
[107] The Free and Hanseatic City of Hamburg v Facebook Ireland Limited, the Administrative Court of Hamburg,15 E 4482/15, Judgment of 3 March 2016.

since *Google Spain*. This resulted in the potential application of the DP laws of multiple Member States to CSPs with branches in multiple member states.[108] This presented compliance problems for especially large multinationals and also indicated potential conflicts as to which state would be the lead regulator. As we shall see below this problem was explicitly dealt with in the GDPR.

2.2.2 Problems in the Case of the Non-EU CSPs regarding to Article 4(1)(c) of the DPD

2.2.2.1 "Equipment"

The DPD did not provide a definition of the term "equipment": what does "equipment" mean exactly? Does it include mobile phones, computers, data centres or local servers used by non-EU CSPs, smart objects attached to the Internet, routers, wires or even data itself. Article 4 (1)(c), tells us that "equipment" does not include tools such as wires merely used for the purpose of the transit of information through EU territory.

The A29WP have argued that all the objects that are used to collect and further process an individual's data in the context of the provision of services in the Internet of Things (IoT) qualify as equipment. "Equipment" thus included devices themselves (e.g. sleep trackers, or watches) and users' terminal devices (e.g. smartphones or computers) and might even include questionnaires and surveys.[109] Particularly, cookies, which are small text files that are downloaded onto terminal devices for collecting and processing data and other similar tracking technology, were also deemed to be equipment.[110]

To conclude, if non-EU CSPs make use of (almost all kinds of) equipment, as mentioned above, which is situated within EU Member State for the processing of personal data in the cloud, the DP law of that Member State would apply to the data processing. This clearly means that the notion of "equipment" has been construed very

[108] See generally in Dan Jerker B. Svantesson, 'Article 4(1)(a) "Establishment of the Controller" in EU Data Privacy Law – Time to Rein in This Expanding Concept?' (2016) 6 IDPL 210.
[109] A29WP, *Opinion 8/2014 on the on Recent Developments on the Internet of Things* (14/EN WP 223, Adopted on 16 September 2014) 10.
[110] See generally in A29WP, *Opinion 1/2008 on Data Protection Issues Related to Search Engines* (00737/EN WP 148, Adopted on 4 April 2008).

broadly.[111]

2.2.2.2 "Make Use of Equipment"

The meaning of "make use of equipment" was left undefined by the DPD. The A29WP also clarified this concept as consisting of two elements:

(i) some kind of activity of the controller;

(ii) the clear intention of the controller to process personal data.[112]

This implies that, if a non-EU CSP places cookies or runs a java script on hard disks of EU users, which are situated within EU Member States, with a view to processing personal data, then this will trigger the application of that Member State's law to the data processing being carried out by such a CSP.[113]

In 2013, the English High Court of Justice held in *Douglas v Hello (No.2)* that there was a processing of unauthorised wedding photographs of Douglas by equipment operating automatically.[114] This processing was used in the transmission by an ISDN line over the internet from a US photographer in New York to London and then sent on to Spain where the Hello magazine containing these photographs was printed. This was making use of equipment in UK which made a US photographer as controller subject to UK DP law.[115]

The connecting factor make use of equipment has been subjected to much criticism as it arguably leads to the possibility of regulatory overreaching.[116] Bygrave is of the view that this ground is expressed so generally and non-discriminatingly that it applies prima facie to a large range of activities without having any realistic chance of being enforced.[117]

---

[111] Lokke Moerel, 'The Long Arm of EU Data Protection Law: Does the Data Protection Directive Apply to Processing of Personal Data of EU Citizens by Websites Worldwide?' (2011) 1 IDPL 28, 33.
[112] A29WP, *Working Document on Determining the International Application of EU Data Protection Law to Personal Data Processing on the Internet by Non-EU Based Web Sites* (5035/01/EN/Final WP 56, Adopted on 30 May 2002) 9.
[113] ibid; A29WP, *Opinion 8/2010 on Applicable Law* (n84) 21.
[114] Douglas V Hello Ltd. [2003] EWHC 786 (Ch), Case No: HCO100644, Judgment of 11 April 2003.
[115] ibid, para 231.
[116] Commission, *Report from the Commission- First Report on the Implementation of the Data Protection Directive (95/46/EC)* (Brussels, 1552003 COM(2003) 265 final) 17.
[117] Bygrave (n88) 8.

For CSPs, the breadth of interpretation was problematic. CSPs often rent the equipment for processing data from other CSPs, who may in turn ultimately use data centres, servers and storage equipment that might be rented from or managed by third parties without knowledge regarding the location of the equipment. Thus the equipment ground might unknowingly subject them to EU DP law.[118]

2.2.3 Does the GDPR Improve the Situation?

2.2.3.1 Extending the Territorial Scope of the EU DP Law to the Processor

The Commission has recognised that the processor also has the ability to exercise control over data processing. The GDPR has made significant changes to the DPD by extending its territorial scope to apply to the processor with a view to providing more protection to personal data, as stated in Article 3(1) that

> This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

This is very crucial for CSPs since they mostly act as processors or sub-processors for the processing of personal data in the cloud. CSPs, will have to become aware for the first time of their obligations and the liabilities which the GDPR imposes directly on them. This might be helpful for addressing the current situation in which the territorial links have been interpreted as far as possible to bring the controllers within the reach of the EU DP law. This means that at least one party (either the controller or the processor) will be responsible for complying with the DP obligations and be liable for the damage caused by their data processing, as set out by the GDPR.

2.2.3.2 New Territorial Links for Non-EU CSPs: Offering and Monitoring

The territorial link that the non-EU controller "makes use of equipment" situated in the

[118] Paul Schwartz, 'Information Privacy in the Cloud' (2013)161 U. Pa. L. Re. 1623,1641.

EU under Article 4(1)(c) of the DPD is replaced by the "offering" and "monitoring" links as stated in Article 3(2) of GDPR that

> This Regulation applies to the processing of personal data of data subjects who are in the Union by *a controller or processor* not established in the Union, where the processing activities are related to:
>
> (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
>
> (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

The "offer" and "monitoring" grounds do seem to be more specific and precise than the "make use of equipment" ground due to the fact that they require some kinds of deliberating targeting. This would make it easier to determine which non-EU CSPs will be obliged to comply with EU DP laws. Nevertheless, these grounds also raise a number of controversial points of interpretation as follows,

(a) "Offering"

There is no definition of "offering" provided by the GDPR. Recital 23 however specifies how to determine whether a controller or processor is offering goods or services to data subjects who are in the EU that [119]

> …it should be ascertained whether it is apparent that *the controller or processor envisages offering services to data subjects* in one or more Member States in the Union. Whereas the *mere accessibility* of the controller's, processor's or an intermediary's website in the Union, of an email address or of other contact details, or the *use of a language* generally used in the third country where the controller is established, is insufficient to ascertain such *intention*, factors such as the use of a language or a currency generally used in one or more Member States with

[119] ibid 3.

> the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union.[120]

Imagine SaaSP B, (a US processor), provides services to the world on the web for a fee using GBP and English language when the page is read from UK ISP's IP address. There is a high probability that its services will be used by UK people. SaaSP B is likely to be caught by the GDPR since SaaSP B makes an obvious offer to UK data subjects.

But imagine SaaS B is built upon a platform supplied by PaaSP A (US sub-processor), which on its on-demand website offers services for a fee using USD and using the English language. It is less obvious that PaaSP A is offering services to UK (or the EU) data subjects and should be subject to the GDPR.

According to Recital 23, there may be evidence of PaaSP A's intention from its use of USD even if its website is accessible to UK B2B customers. Arguably, English may be used as an international language. On the other hand, any currency could be translated if users use credit cards or Paypal so it might be foreseeable for PaaSP A that its service will be used by any users, including UK users. This leads to the questions:

(1) Should we enforce the EU DP law against this US based PaaSP A, who does not know whether its service will be offered to UK people?

(2) Can PaaSP A avoid these EU DP obligations by using a contract to force SaaSP B to do all the compliance with the EU DP law? Are there any liabilities falling on PaaSP A?

There are relevant cases here relating to "directing" online commercial activities to consumers regarding Article 15 of Regulation (EC) No 44/2001.[121] These cases on jurisdiction in consumer contracts are worth considering.

---

[120] GDPR, Rec 23.

[121] The court of the consumer's Member State will have jurisdiction if such a party pursues commercial or professional activities in the Member State of the consumer's domicile or, by any means, directs such activities to that Member State or to several States including that Member State. See Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, Art 15.

The CJEU handed down a landmark decision in the 2010 case *Peter Pammer v Reederei Schlüter and Hotel Alpenhof v Oliver Heller*.[122] The defendant, Oliver Heller, domiciled in Germany, was making his reservation from Hotel Alpenhof in Austria by using the email address indicated on the Hotel's website. When he arrived, he found fault with the rooms and left without paying his bill. The hotel then brought an action before an Austrian court for payment. Mr. Heller argued that as a consumer domiciled in Germany, he could be sued only in the German court.

The CJEU held that it was for the national court to ascertain whether the trader envisaged doing business with consumers domiciled in German by considering a provided list of matters that were capable of constituting such directing activities as follows,

(1) the international nature of the activity;

(2) the mention of itineraries from other Member States for going to the place where the trader is established;

(3) the use of a language or a currency other than the language or currency generally used in the Member State in which the trader is established with the possibility of making and confirming the reservation in that other language;

(4) the mention of telephone numbers with an international code, outlay of expenditure on an internet referencing service in order to facilitate access to the trader's site or that of its intermediary by consumers domiciled in other Member States;

(5) the use of a top-level domain name other than that of the Member State in which the trader is established; and

(6) the mention of an international clientel composed of customers domiciled in various Member States.[123]

The court also indicated that the mere accessibility of the trader's or the intermediary's website in the Member State where the consumer was domiciled was insufficient to imply that the trader was directing its activity to the State of the

[122] Joined Cases C-585/08 Peter Pammer v Reederei Karl Schlüter GmbH & Co KG and C-144/09 C Hotel Alpenhof GesmbH v Oliver Heller, Judgment of 7 December 2010.
[123] ibid para 93.

consumer's domicile.[124] The same went for (1) the mention of an email address and of other contact details, (2) the use of a language or a currency which are the language and/or currency generally used in the member State in which the trader is established.[125]

Another relevant question is whether an offer needs to be accepted by data subjects in the EU? Since a payment of data subjects in the EU, which is an action showing the acceptance of data subjects, is not required by Article 3(2)(a), the acceptance might not be needed for bringing non-EU CSPs within the reach of EU DP law. Arguably, it might be quite broad to enforce the EU DP law on all CSPs who just offer their services to data subjects in the EU. There might be at least some activities expressing the fact that data subjects intend to use goods or services offered by non-EU CSPs.

(b) "Monitoring"

The GDPR also does not provide a definition of "monitoring".[126] Recital 24 however notes that "monitoring" will occur where

> …natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of *profiling* a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes

The GPDR equates the concept of "monitoring" of behaviour broadly with "profiling".[127] Therefore, when non-EU CSPs carry out the monitoring of people within the EU, such as by profiling individuals, including analysing or predicting their performance at work, their health, personal preferences or interests (e.g. web analytics

[124] ibid para 94.
[125] ibid.
[126] ICO, *Proposed New EU General Data Protection Regulation: Article-by-Article Analysis Paper* (V10 12 February 2013) 5.
[127] GDPR, Art 4 (4) defines profiling as

> any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

companies), even if they do not make any online sales to them, these CSPs might be subject to the EU DP law.

Imagine an African based charity which makes money by putting out advertisements targeting UK data subjects via Facebook. The charity will arguably be subject to the EU DP law because it monitors the behaviour of UK data subjects under Article 3(2)(b) of the GDPR. However, the question arises as to whether this is how it works when the charity does not themselves monitor the behaviour of EU data subjects, but gets a processor to do it. For example, if the charity puts out an advertisement via Google Adwords, Google is likely to do the majority of the profiling and furthermore the advertisement may or may not come up in the UK or in the EU at all: it depends how the advertising dashboard was set up. The charity does not necessary know whether Google intentionally monitors the behaviour of UK data subjects, it just pays Google for displaying its advertisement to the web users. Should it fall under the regulation of the EU DP law? (The question is likely to be unnecessary to answer though since if the charity has offers goods or services to the UK people, as opposed to simply advertising to build brand, it would still be caught by the EU DP law under Article 3(2)(a) of the GDPR).

The "monitoring" ground may go too far in applying EU DP law to non-EU CSPs in circumstances where the monitoring does not actually affect the privacy rights of EU data subjects. The charity example above may show this: Schwartz argues that merely observing without making any decision about a person should not be regulated by the EU DP law[128] There are situations where information is collected about EU users by service providers for aggregate good e.g. the collection of information to prevent unsafe browsers from logging on to cloud services.[129]

2.2.3.3 Separate Rule for Identifying the Applicable Law

The rules for determining territorial scope and applicable law, which were previously mixed up in Article 4 of the DPD, are separated by the GDPR. While the GDPR sets out

[128] ibid.
[129] Paul M. Schwartz, 'EU Privacy and the Cloud: Consent and Jurisdiction Under the Proposed Regulation' (2013) 12 PVLR 718, 720.

the rule about its territorial scope in Article 3, it simply refers the rule about the applicable law to Article 56, which mainly provides the rule for identifying which Member State's supervisory authority has jurisdiction where CSPs have multiple establishments within the EU as stating that

> the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor...[130]

In cases involving both the controller and the processor, the GDPR indicates that the lead DPA should be the DPA of the Member State where the controller has its main establishment.[131] The GDPR also provides a definition of "the main establishment" of the controller as

> the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment.[132]

and that of the processor as

> the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation.[133]

Moreover, the GDPR further clarifies in Recital 36 that the main establishment of a

[130] GDPR, Art 56(1).
[131] GDPR, Rec 36.
[132] GDPR, Art 4(16)(a).
[133] GDPR, Art 4(16)(b).

controller relates to the "effective and real exercise of management activities" that determine the main decisions regarding the purposes and means of processing through "stable arrangements". Whether the processing of personal data is carried out at that location is not necessary and the presence and use of technical means and technologies for processing personal data do not, in themselves, constitute the main establishment.[134] The presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute a main establishment and they are not determining criteria for a main establishment.[135] Therefore, when EU CSPs have their establishments in more than one EU Member State, the DP law of the jurisdiction of their lead DPA will apply. The rule in Article 56 is known as the "one stop shop".

The rules about the applicable law for non-EU CSPs, are referred to Article 27, which is mainly about appointing representatives of the non-EU controller and processor in the EU after they have been caught by the territorial scope in Article 3(2) of the GDPR. Article 27(2) states that

> The representative shall be established in one of the Member States where the data subjects, whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, are.

Thus, non-EU CSPs will be subject to the law of the Member State in which the CSPs offers goods/ services or monitors EU users. These CSPs must appoint their representatives in those States to act on their behalf with regard to their obligations and to be subject to enforcement proceedings in the event of non-compliance by CSPs.[136] This would be convenient for EU data subjects to enforce their rights against non-EU CSPs.

2.2.4 Conclusions

Article 4 of the DPD worked well to protect EU data subjects even where their data were processed by non-EU CSPs; but failed in the goal to prevent a situation where the CSP

[134] GDPR, Rec 36.
[135] ibid.
[136] GDPR, Rec 80.

was governed by the laws of more than one Member State.

The rule for determining territorial scope and applicable law, which were previously mixed up in the DPD, have been separated by the GDPR. This should make it easier to identify whether EU DP law applies to data processing in the cloud; and which DP Member State laws apply to such data processing.

In the case of EU CSPs, the expansion of the territorial scope of the EU DP law resulting from a very wide interpretation of the phrase "in the context of the activities of such an establishment" in the DPD by the courts, does raise many controversial issues. The GDPR further expands these difficulties for CSPs by extending its territorial scope to cover the processor. For EU data subjects, this means they can be sure that there will be at least one CSP to comply with the DP obligations under the EU DP law to protect their rights. But CSPs, particularly processors, will have to become aware of their compliance duty with regard to the EU DP law. The GDPR addresses the situation where CSPs are subject to multiple and potentially conflicting rules of different nations' DP laws by introducing the "one stop shop" rule. Nevertheless, how effective this rule will be in practice in the cloud is the subject of considerable debate.

The GDPR also redefines the concept of the main establishment of the controller and processor, which is relevant to the applicable law rather than the territorial scope. This still leaves the situation difficult for CSPs who have more than one establishment. Bygrave suggests that this might be remedied if the applicable law were to be made the law of the Member State where a data subject has his/her domicile, which is parallel with the rule on the choice of law in consumer contracts.[137].

In the case of non-EU CSPs, the DPD marked a significant extension of the extraterritorial application of the EU DP law, resulting from the very broad definition of "making use of equipment". The GDPR deals with this situation by removing the notion of equipment and introducing the new connecting factors of "offering" and "monitoring". Both appear to be more precise than the previous, which would provide more certainty about the law to CSPs.

The GDPR does seem to reflect an increasingly globalised world with data being

[137] Bygrave (n88) 10.

transferred in and out of jurisdictions more than the DPD did. In the next section, the author looks at the third key problem, which relates to whether personal data can legally be exported from the EU to their clients and data centres located outside the EU.

2.3 Data Export Rules: Can Personal Data Held in Cloud Computing be Transferred into the Non-EU Cloud Computing?

In order to achieve a balance of interests between the protection of personal data and facilitating the free flow of personal data, the DPD set out the data export rules which prohibited the transfer of personal data outside the EU, with some exceptions.[138] The underlying concept of data export rules is to provide an adequate level of protection to personal data transferred outside the EU, similar to (though not necessarily identical) to that provided within the EU. This section will discuss the problems that are created when applying the data export rules to cloud computing, before analysing whether they can be addressed by the GDPR in the following section.

2.3.1 Which Circumstances Will Amount to a Data Transfer in the Cloud?

CSPs typically offer automated data transfer, and such transfer often involves data centres in various different locations, including both within and outside the EU.[139] The first question is whether these automated transfers are subject to the data export rule under the DPD.

What is meant by "data transfer", has not been clarified by the DPD. *Lindqvist* in 2003 indicated that there is no data transfer outside the EU when uploading personal data on to a public internet page, which makes data accessible to anyone who is connected to the Internet, including non-EU people.[140] This was justified on the grounds that the data was not directly transferred by the data controller outside the EU but went through the computer infrastructure where the page was stored.[141]

Hon et al suggest this implies that "data transfer" should be based on an "intention" to give or allow logical access to intelligible personal data to a third party

[138] DPD, Art 25-26.
[139] Frank Alleweldt and others, *Cloud Computing* (European Parliament's Committee on Internal Market and Consumer Protection, 2012) 82.
[140] Case C-101/01 Bodil Lindqvist [2003] ECR I-12971, Judgment of 6 November 2003, Para 69,71.
[141] ibid.

recipient.[142] Thus, an *automated* transfer of the personal data between the data centres of one CSP, may not constitute a "data transfer". Arguably, it may be an intention of the one who organises automation or there is an uploading of personal data with non- EU CSP who has various data centres located outside the EU. If it is reasonably foreseeable that such data can be transferred outside the EU, such automated data transfer is likely to constitute a data transfer which is subject to the data export rule.

Another problem is when non-EU CSPs transfer data to other non-EU CSPs, which is known as "onward transfer", it is unclear whether this onward transfer is a subset of "data transfer" under the DPD and subject to the data export rule. The A29WP opined that

> further transfers of the personal data from the destination third country to another third country should be permitted only where the second third country also affords an adequate level of protection, the only exceptions permitted should be in line with art 26 of the DPD.[143]

This is very important for CSPs due to the fact that there is multiplicity of possible architectures of cloud services. Many CSPs operating in the EU use chains of sub-processors as discussed earlier some of whom may be outside the EU and make onward transfers between each other. CSPs may not know the details of these onward transfer and it may be quite difficult in practice for these CSPs to ensure compliance with the data export rule if it is applied to onward transfers. Contracts requiring certain obligations be put on sub-contractors seem to be the best option to avoid the risk of breaching the data export rule e.g. including requirements to notify who the sub-processor is and where the sub-processor is located. Another solution, which has become popular among CSPs, is a regional cloud, in which CSPs offer users the option to select the location for their data/ application to be stored or processed.[144]

---

[142] W Kuan Hon and Christopher Millard, 'How Do Restrictions on International Data Transfers Work in Clouds? ' in Christopher Millard (ed), *Cloud Computing Law* (OUP 2013) 259.
[143] A29WP, 'First Orientations on Transfers of Personal Data to Third Countries - Possible Ways Forward in Assessing Adequacy' XV D/5020/97-EN final WP4, 26 June 1997.
[144] See Amazon Web Service and Google Cloud Platform, <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html> and

2.3.2 Grounds for Lawful Transfer of Personal Data in the Cloud Outside the EU

The DPD allowed the transfer of personal data to non-EU countries if

(1) those countries ensured an adequate level of DP – the European Commission is competent to assess the level of DP in foreign countries through adequacy findings and consults on the assessment with the A29WP which has substantially contributed to the interpretation of Articles 25 and 26. or; [145]

(2) a derogation applied, e.g. the data subject's consent or standard contractual clauses (SCCs)[146] or;

(3) there was an adequate safeguard adduced by the controllers, e.g. through BCRs or the EU-US Safe Harbor Agreement. [147]

In practice, a number of problems made these grounds for transfer outside the EU difficult to apply in the cloud as follows,

2.3.2.1 Problems with Consent

Article 26(1)(a) of the DPD allowed personal data to be exported to third countries if the data subject has given "unambiguous consent" to a data transfer, regardless of the lack of adequate protection. "Unambiguious consent" was not precisely defined but the DPD did mention "explicit consent" as a requirement for the processing of sensitive personal data.[148] "Consent" was defined generally in Article 4(h) as

> any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

<https://cloud.google.com/storage/docs/bucket-locations access> accessed 15 March 2018; For exmaple, German requires government cloud services to only store personal data in Germany (German Federal Cloud which is callled "Bundescloud")

[145] DPD, Art 25(1).
[146] DPD, Art 26(1)(a) and 26(2).
[147] DPD, Art 26(2).
[148] DPD, Art 8(2)(a).

This consent is composed of four main elements.[149]

(1) *It must be freely given* - consent should result from the free choice of an individual, free from external manipulations. Consent cannot be freely given where there is an imbalance of data subjects and CSPs.[150] Whether or not consent is freely given when cloud users accept a standard form of cloud contract which is based on a "take it or leave it" approach remains unclear.

(2) *It must be specific* – consent should be based on the concept of specify, purpose limitation, and proportionality.[151] Regarding the case of *Deutsche Telekom AG v Bundesrepublik Deutschland*, the CJEU held in 2011 that the renewed consent of the data subject is not needed, if the data subject had been informed in the past about a specific data processing of his personal data.[152] But it remains unclear whether the consent given by the data subject for every operation as stated in the contract, is specific.

(3) *It must be informed* – the data subject must be properly informed by a precise and intelligible notice in which transparency is promoted to allow the data subject to control data. The data subject must understand the fact and the implication of the processing activities performed upon their data.[153] The question remains how much information is needed.

(4) *It must signify* – there must be at least some actions of the data subject to signify their agreements relating to personal data processing, such as clicking on an "I agree" button to accept the terms and conditions. A "browse wrap contract", in which no "I agree" button is provided, may lack consent .[154]

After all this, what is the difference between general, explicit and unambiguous

[149] Maurizio Borghi, Federico Ferretti and Stavroula Karapapa, 'Online Data Processing Consent Under EU Law: a Theoretical Framework and Empirical Evidence from the UK' (2013) 21 IJLIT 109, 120-6.
[150] A29WP and WPPJ, 'The Future of Privacy : Joint Contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data' 02356/09/EN, WP 168 Adopted on 01 December 2009, 17.
[151] Yves Poullet and J. Marc Dinan, 'The Internet and Private Life in Europe: Risks and Aspirations' in Andrew T Kenyon and Megan Richardson (eds), *New Dimensions in Privacy Law* (CUP 2006) 60, 62.
[152] Case C‑543/09 Deutsche Telekom AG v Bundesrepublik Deutschland, CJEU, Judgment of 5 May 2011, para 65,67.
[153] Deryck Beyleveld and Roger Brownsword, *Consent in the Law* (Hart Publishing 2007) 9.
[154] Elizabeth Macdonald, 'When is a Contract Formed by the Browse-Wrap Process?' (2011) 19 IJLIT

consent remains far from clear. The Commission recognised that the concept of "unambiguous consent", as compared with "explicit consent", needed further clarification and a more uniform interpretation'.[155] The A29WP suggests that "unambiguous consent" must leave no doubt as to the data subject's intention and must enable the data subject to give at least some kind of "active indication" of their wishes.[156] It must be clear and conclusive, the absence of behaviour or passive behaviour is thus generally insufficient to constitute valid consent. But it might be sufficient when it includes some sort of action which needs to be considered case by case.[157] This question arises as to whether opt-out consent, which enables the automatic processing of data unless a data subject explicitly objects to such processing, fall under the meaning of "unambiguous consent".[158]

Apart from that, the use of consent to achieve compliance with the data export rule does not seem to be an effective approach for safeguarding the data subject's privacy.[159] The nature of consent is designed for specific one-off transfers, so that it would be unsuited to the nature of cloud computing, which always involves the repeated or ongoing exchanges of personal data.[160] Moreover, there are often a multiplicity of players (sub-CSPs or sub-sub-CSPs), involved in the same set of personal data processing in the cloud, and some of whom may not have any direct relationship with each other, the amount of knowledge in terms of who is the data subject from whom consent must be obtained to validate the data transfer is quite low.[161] Furthermore, since there is no possibility of negotiating a cloud contract, consents given by individual cloud users do not seem to be meaningful. Accordingly, consent has been subjected to much

[155] Commission, *Report from the Commission- First Report on the Implementation of the Data Protection Directive (95/46/EC)* (n116).
[156] A29WP, *Opinion 15/2011 on the Definition of Consent* (01197/11/EN WP187, Adopted 13 July 2011) 12 and 21.
[157] Eleni Kosta, *Consent in European Data Protection Law* (Martinus Nijhoff 2013) 188.
[158] ibid; Kuner, *European Data Protection Law : Corporate Compliance and Regulation* (n28) para 2.17.
[159] Hon and Millard 'How Do Restrictions on International Data Transfer Work in the Cloud' in Millard C (ed) (n142) 261.
[160] Judith Rauhofer and Casper Bowden, 'Protecting Their Own:Fundamental Rights Implications for EU Data Sovereignty in the Cloud' (Edinburgh School of Law Research Paper Series No 2013/28) 5.
[161] A29WP, Opinion 05/2012 on Cloud Computing (n43) 17; J. Nancy King and V.T. Raja, 'What Do They Really Know About Me in the Cloud? A Comparative Law Perspective on Protecting Privacy and Security of Sensitive Consumer Data' (2013) 50 Am Bus LJ 413, 435.

criticism as to whether it is "meaningful" and if it actually creates user control in practice.[162]

2.3.2.2 Problems with Standard Contractual Clauses (SCCs)

Article 26(2) allows data transfers, which are made via SCCs approved by the Commission. Some Member States also require prior notification to and/or approval by their home DPA before model clauses can be used.[163] These clauses have been being used for example by Microsoft and Google.[164]

There are two type of SCCs approved by the Commission:

(1) SCCs for data transferring from EU controllers to non-EU controllers (adopted in 2001 and then revised in 2004); [165]

(2) SCCs for data transferring from EU controllers to non-EU processors (adopted in 2002).[166] Then, it was revised in 2010 to allow non-EU processors to subcontract with other non-EU sub-processors or sub-sub processor. This sub-processing requires prior written consent of an EU controller, while a non-EU processor must put in place a written agreement with each sub-processor that mirrors the terms of "controller to processor", which is subject to a contractual obligation to provide an adequate level of protection in respect to the EU DP law.[167]

---

[162] Daniel J. Solove, 'Introduction: Privacy Self-Managemen and the Consent Dilemma' (2013) 126 Harv L Rev 1880, 1897; A29WP, *Working Document on a Common Interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995* (Adopted on 25 November 2005, 2093/05/EN WP 114).

[163] DPD, Rec 59-60 and Art 26(2)-(4), 31(2).

[164] The EU DPA approved the contractual commitment of both Microsoft Cloud (2014) and Google Cloud (2017) as they are inline with the SCCs approved by the Commission.
See 'EU Data Protection Regulator Says Microsoft Enterprise Cloud Contracts are in Line with EU Privacy Requirements' (2014) <https://www.microsoft.com/en-us/TrustCenter/Compliance/EU-Model-Clauses> accessed 1 January 2017; Google Cloud, 'EU Data Protection Authorities Confirm Compliance of Google Cloud Commitments for International Data Flows' (2 February 2017) <https://blog.google/topics/google-cloud/eu-data-protection-authorities-confirm-compliance-google-cloud-commitments-international-data-flows/> accessed 1 March 2017.

[165] Paolo Balboni, *Trustmarks in E-Commerce: The Value of Web Seals and the Liablity of Their Providers* (T.M.C Asser Press 2009); *Commission Decision of 27 December 2004 Amending Decision 2001/497/EC as Regards the Introduction of an Alternative Set of Standard Contractual Clauses for the Transfer of Personal Data to Third Countries* ((2004/915/EC) 29 December 2004, L 385/74.

[166] David G. Carnevale, *Trustworthy Government : Leadership and Management Strategies for Building Trust and High Performance* (San Francisco : Jossey-Bass 1995).

[167] *Commission Decision of 5 February 2010 on Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries under Directive 95/46/EC of the European Parliament and of the Council* ((2010/87/EU) 12 Febuary 2010, L39/5) (17).

The use of all these clauses is very crucial for the cloud as a mechanism for safeguarding DP rights of EU data subjects in the cloud. Nevertheless, there are many issues that prevent them from working effectively to serve that protection.

Firstly, the existing clauses are limited and inflexible as to the actors and the circumstances they involve. As has been discussed in section 2.1, the position of CSPs is uncertain. They could be either processors or controllers, or both processors and controllers or nothing for the same set of data processing. Additionally, there might be more than one CSPs involved in the same data processing which might have their establishments located outside the EU.

The existing model clauses do not fully cover all scenarios of data transfer in the cloud, e.g. data transfer between non-EU controllers to non-EU processors when the initial controller is in the EU.[168] Alternatively, EU controllers would need to either have a direct contract with such non-EU processors (EU controllers might be reluctant to enter into contractual relationships with such non-EU processors that they have never contracted with before) or to authorise non- EU controllers to subcontract with such non-EU processor /sub-processors on its behalf, and such non-EU processor /sub-processors would have to incorporate those model clauses.

Secondly, many Member States, e.g. Austria and Spain, require prior approval from the relevant local DPA (in the country of the data exporter) for a data transfer which is based on SCCs.[169] It would not be convenient for CSPs to apply for approval from a different local DPA, particularly for multinational companies.

Lastly, there have been more challenges for SCCs in 2016 when its validation has been challenged by the Irish DPC, as part of the investigation concerning the case of *DPC vs Facebook Ireland and Schrems*.[170] In April 2018, the Irish DPA have just referred this case to the CJEU to make a ruling on the validation of SCCs by

[168] Hon and Millard 'How Do Restrictions on International Data Transfer Works in the Cloud' (n142) 271-272.
[169] Norton Rose Fulbright, 'Global Data Privacy Directory' (*July 2014*) <http://www.nortonrosefulbright.com/files/global-data-privacy-directory-52687.pdf> accessed 1 March 2017.
[170] Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, No 4809 P, High Court of Ireland, judgment of 19 July 2016.

determining whether transfers of personal data from the EU to the US pursuant to the SCCs provide adequate level of DP for EU data subjects against US government surveillance.[171] As long as far-reaching US surveillance laws still exist, the CJEU is very likely to declare that the transfers to the U.S. based on SCCs are vitiated for the same reasons as those relating to the invalidation of the Safe Harbor regime.[172]

2.3.2.3 Problems with Binding Corporate Rules (BCRs)

BCRs are meant to be used by multinational companies for international data transfer within the same corporate group, regardless of the location of their establishments. Although BCRs are not explicitly recognised in the DPD, the Member State DPA recognised them as a legal basis for international data transfer under Article 26(2) of the DPD. They are subject to the authorisation of the relevant national DPA, with the support of A29WP.[173]

There are two main types of BCRs;

(1) BCRs for controllers, which are intended to regulate the data transfer that is originally performed by a company as a controller within the same corporate group, e.g. within a group of private cloud;[174]

(2) BCRs for processors, which are intended to regulate the data transfer that is originally processed by a processor on behalf of an EU controller under its instruction (requiring prior information to and prior written consent from the controller) to a sub-processor within the same corporate group of processors. In May 2015, A29WP issued a new guideline allowing company to subcontract its obligations to an external sub-processor with the prior consent of controller by way of a written agreement and such

[171] Commission, *Communication from the Commission to the European Parliament and the Council: Exchanging and Protecting Personal Data in a Globalised World* (Brussels, 1012017, COM(2017) 7 final).
[172] See more detailed discussion of this in chapter 4.
[173] See a list of A29WP working papers on BCRs, at < http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/tools/index_en.htm > accessed 1 April 2018.
[174] A29WP, *Working Document Setting up a Table with the Elements and Principles to be Found in Binding Corporate Rules* (1271-00-00/08/EN WP 153, Adopted on 24 June 2008); A29WP, *Working Document Setting up a Framework for the Structure of Binding Corporate Rules* (1271-00-01/08/EN WP 154, Adopted on 24 June 2008); A29WP, *Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules* (1271-04-02/08/EN WP 155 rev04, Adopted on 24 June 2008 as last Revised and adopted on 8 April 2009).

sub-processor will have to put in place BCRs for processor as it is a sister company of processor.[175]

BCRs do not seem to be useful in the cloud. This is because the use of BCRs would not scale well to the data transfer within the cloud where many CSPs who involve the same set of data transfer is uncertain, is a controller or processor or nothing.[176] Furthermore, BCRs have to be accepted by a lead DPA, and after that the company has to apply for further authorisation to all relevant DPAs in accordance with the applicable national law.[177] Since different Member States have their own approval procedures and there might be some difficulties where local laws conflict with the way in which a company has approached the BCR, implementing BCRs are in practice quite cumbersome, expensive and time-consuming.[178]

2.3.2.4 Problems with the EU–US Safe Harbor Agreement

The Safe Harbor regime is a system designed to facilitate the transfer of personal data from the EU to the US. It was based on self regulation and is discussed in detail in the next chapter. Dissatisfaction has been expressed with the actual operation of the Safe Harbor regime in providing a good level of protection to personal data exported to the US by academics and the Commission - for instance many self-certified organisations that have not published a privacy policy with regard to data processing adhering to the Safe Harbor principles or have published a policy that is not compliant with the Safe Harbor principles.[179] The reviews of Safe Harbor by the Commission have shown that it is seen as a poor mechanism for bridging the gap between EU and US DP norms.[180] Moreover, it was found that many US businesses were making false claims of Safe

[175] A29WP, *Explanatory Document on the Processor Binding Corporate Rules* (00658/13/EN WP 204 rev01, Adopted on 19 April 2013 As last revised and adopted on 22 May 2015) 7- 9.
[176] See section 2.1.
[177] A29WP 'BCRs Procedure'<http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/procedure/index_en.htm> accessed 1 March 2018.
[178] Christopher Kuner, *European Data Protection Law : Corporate Compliance and Regulation* (n28) 4.120-4.154 ;Lokke Moerel, *Binding Corporate Rules: Corporate Self-Regulation of Global Data Transfers* (OUP 2012) 6.6.1; ICO, 59.
[179] Commission, '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' (n19) 14.
[180] ibid.

Harbor certification.[181] Scholars have suggested that EU data exporters should not merely rely on evidence of Safe Harbor self-certification and evidence demonstrating that their principles are compliant with the Safe Harbor rules, but should also ask for additional safeguards, e.g. SCCs or BCRs for ensuring an adequate level of DP.[182]

Especially since the Snowden revelations in 2013 about mass surveillance by NSAs and LEAs (see chapter 4, section 1.3.3), doubts became profound about the effectiveness of the Safe Harbor regime.[183] Finally, on 6 Oct 2015, the CJEU made a decision in the case of *Maximillian Schrems v Data Protection Commissioner*, that the Safe Harbor agreement was invalid.[184] The court held that the US did not afford an adequate level of DP because the national security, public interest and law enforcement requirements of the US prevailed over the Safe Harbor scheme. Thus, US businesses were bound to disregard, without limitation, the protective rules laid down by that scheme.

This decision was cataclysmic for business, especially for cloud computing. Alternative exceptions for justification of the transfer of personal data outside the EU were sought.[185] A renewed and sound approach for transatlantic data flows which meet the criteria established in the *Schrems* decision is now required.[186] Many CSPs, e.g. Google, IBM, Microsoft and Amazon, have sought to build data centres in the EU with a view to rebuilding trust among EU data subjects or businesses since they ensure that user data will stay within EU territory.[187]

2.3.3 Does the GDPR Improve the Situation?

2.3.3.1. New Scope of the Data Export Rule

[181] FTC, *Court Halts U.S. Internet Seller Deceptively Posing as U.K. Home Electronics Site* (FTC File No 092-3081, 6 August 2009).
[182] A29WP, *Opinion 05/2012 on Cloud Computing* (n43) 17; Mike Ewing, 'The Perfect Storm: The Safe Harbour and the Directive on Data Protection' (2002) 24 Hous J Int'l L 315.
[183] See more details in chapter 4.
[184] Case C-362/14 Maximillian Schrems v Data Protection Commissioner [2015] CJEU No. 117/15, judgment of 6 October 2015.
[185] See more details in chapter 4.
[186] Voss WG, 'The Future of Transatlantic Data Flows: Privacy Shield or Bust?' (2016) 19 J Internet L 8.
[187] Archana Venkatraman, 'Cloud Providers Rush to Build European Data Centres over Data Sovereignty' (*14 October 2014*) <http://www.computerweekly.com/news/2240233331/Cloud-providers-rush-to-build-European-datacentres-over-data-sovereignty> accessed 1 January 2017.

The GDPR extends the scope of the data export rule in the DPD to apply to processors and it also expressly covers the case of "onward transfer" of personal data. Article 44 states that

> any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if… the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation.[188]

It has not yet provided a definition of "data transfer", but it defines in Recital 101 an "onward transfer" as involving the circumstances of

> any transfers of personal data from the third country or an international organisation to controllers, processors in the same or another third country or international organisation.[189]

Accordingly, it is now clear that when non-EU CSPs transfer personal data to other non-EU CSPs in the same or another non-EU country, when the initial controller is in the EU, such data transfers will be subject to the data export rule under the EU DP law. CSPs will now have to be more aware about the place where the data will be stored or processed in sub-chains of processors. Contracts with sub-CSPs will have to take this into account so as to ensure compliance with the data export rule.

2.3.3.2 Grounds for Lawful Transfer of Personal Data in the Cloud Outside the EU

The GDPR retains most of the circumstances allowing for data transfer outside the EU in the DPD with some changes, including

(1) it provides more details about how the Commission should determine when

[188] GDPR, Art 44.
[189] GDPR, Rec 101 and Art 44.

non-EU countries have an adequate level of DP.[190]

(2) if no adequacy decision has been made, it introduces some new alternative safeguards to legalise data exports to that country, which do not require any specific authorisation from a DPA. These now include:

(a) a legally binding and enforceable instrument between public authorities or bodies[191];

(b) BCRs in accordance with Article 47[192];

(c) SCCs adopted by a DPA and approved by the Commission[193];

(d) an approved code of conduct[194];

(e) an approved certification mechanism.[195]

(3) it introduces new alternative safeguards to an adequacy decision, which *are* subject to authorisation from a competent DPA. These now include:

(a) SCCs between the controller or processor and the controller, the processor or the recipient of the personal data in the third country or international organisation[196];

(b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.[197]

(4) it introduces a new ground for data transfer which is a response to the judgment of a court or tribunal and any decision of an administrative authority of non-EU countries, which is based on an international agreement.[198]

(5) it makes some changes to the current derogations:

(a) it requires an explicit consent rather than an unambiguous consent, as was the case in the DPD, after the data subject has been informed of the possible risks of

[190] GDPR, Art 45.
[191] GDPR, Art 46(2)(a).
[192] GDPR, Art 46(2)(b) and 47.
[193] GDPR, Arts 46(2)(d) and 93(2).
[194] GDPR, Arts 40 and 46(2)(e).
[195] GDPR, Arts 42 and 46(2)(f).
[196] GDPR, Arts 46 (3)(a).
[197] GDPR, Arts 46 (3)(b).
[198] GDPR, Arts 48.

such transfers[199];

(b) it retains the circumstance when the data transfer is necessary for important reasons of the public interest, but further requires that such interests must be recognised in EU law or in the law of the Member State to which the controller is subject[200];

(c) it extends the scope of the circumstance when the data transfer is necessary in order to protect the vital interests of the data subject to cover the vital interests of other persons, where the data subject is physically or legally incapable of giving consent.[201]

2.3.3.2.1 Replacing Unambiguous Consent with Explicit Consent

The GPDR makes some changes to the consent ground for the lawful transfer of personal data outside the EU in the DPD by (1) replacing the "unambiguous" consent of the data subject in the DPD by "explicit" consent;(2) further requiring that the data subject should have been informed of the possible risks of the data transfer before giving consent.[202]

The GDPR also provides a slightly amended definition of consent in Article 4(11) that

> any freely given and specific, informed and *unambiguous* indication of the data subject's wishes by which he or she, *by a statement or by a clear affirmation action*, signifies agreement to the processing of personal data relating to him or her.

Compared with the DPD, this is clearer on what constitutes consent, since the new definition explicitly specifies in what ways consent can be given, which is either "*by a statement or by a clear affirmation action"*.

Recital 32 further clarifies how a statement or a clear affirmation action can be given as

[199] GDPR, Arts 49 (1)(a).
[200] GDPR, Arts 46 (1)(d).
[201] GDPR, Arts 46 (1)(f).
[202] GDPR, Arts 49(1)(a).

> …by a written statement, including by electronic means, or an oral statement and that in an online consent can be given by ticking a box when visiting an internet website but silence, pre-ticked boxes or inactivity should not therefore constitute consent.

Therefore, it is now clear that there must be at least some activity of the data subjects clearly indicating their consent and the absence of action of the data subject does not constitute consent.

When the data subject's consent is given by a written declaration, the GDPR specifically requires that the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an *intelligible* and *easily accessible* form, using *clear and plain language*.[203] If this is not the case, the consent given by the data subject will not be valid and the controller or processor who makes a request will be subject to an administration fine under Article 83(5)(a).[204]

Apart from that, the GDPR tries to clarify the elements of general consent (Article 4(11)) as follows:

(1) *it must be freely given* - consent will not be regarded as freely given where

(a) the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.[205]

(b) there is a clear imbalance between the data subject and the controller.[206]

(c) separate consent cannot be given to different personal data processing operations despite its being appropriate in the individual case.[207]

(d) the consent to the data processing is a prerequisite for the performance of a contract, including the provision of a service, for which the consent is not necessary for the performance of that contract.[208]

---

[203] GDPR, Rec 42 and Art 7(2).
[204] GDPR, Art 83(2) and Art 83(5)(a). It is subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.
[205] GDPR, Rec 42 and Art 7(3).
[206] GDPR, Rec 43.
[207] GDPR, Rec 43.
[208] GDPR, Art 7(4).

(2) *it must be specific* - consent must be obtained in a manner that is distinguishable from other matters. Consent should cover all processing activities carried out for the same purpose or purposes, so that when the processing has multiple purposes, consent should be given for all of them.[209]

(3) *it must be informed* - the data subjects must be informed of their rights to withdraw consent at any time prior to giving consent.[210]And the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended.[211]

It can be argued that a cloud contract which is based on a "take it or leave it" approach is arguably not valid under the GDPR due to the fact that (1) individual cloud users do not always have an ability to negotiate with CSPs;(2) they do not seem to have a free choice to refuse or withdraw their consent; and (3) consent given by cloud users is often for all of the processing activities, not limited to a specific context. All these could potentially have a huge impact on a business to consumer(B2C) contract in an online since it has been routinely done in a standard form including terms and conditions which always express in favour of businesses. The GDPR will probably make it more difficult to obtain valid consent from the data subject, with the result of greatly limiting its availability for cloud computing.[212]

In the particular case of consent as a legal justification for data export, the GDPR places many more restrictions than was the case under the DPD:

(1) the data subject must explicitly provide consent to the data transfer.[213] This may have significant implications for cloud services, e.g. by requiring an increased use of pop-up boxes and other mechanisms on web sites. The shift from "unambiguous" consent to "explicit" consent might not however make very much practical difference to

[209] GDPR, Rec 32 and Art 7(2).
[210] GDPR, Art 7(3).
[211] GDPR, Rec 42.
[212] Claudia Quelle, 'Not Just User Control in the General Data Protection Regulation On the Problems with Choice and Paternalism, and on the Point of Data Protection' in Anja Lehmann, Diane Whitehouse and Simone Fischer-Hübner (eds), *Privacy and Identity Management Facing up to Next Steps*, vol 128 (Springer 2017) 140-163 and 145.
[213] Christopher Kuner, *The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law* (Bloomberg BNA Privacy and Security Law Report 6 February 2012) 9-10.

secure the apparent objective of genuine consent in an online environment.[214]

(2) the data subject must be informed about the possible risks associated with the data transfer before giving consent. Article 7 of the GDPR clearly states that the controller is obliged to demonstrate that the data subject has consented to the processing of his or her personal data and presumably this includes being able to demonstate that risks were explained. Again, this obligation could potentially impose increased costs and administrative burdens on CSPs to fulfil it.[215]

(3) Crucially, the GDPR provides that the consent derogation should be applicable solely to the data transfer that is 'not repetitive and concerns only a limited number of data subjects' or 'is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject'. [216] Therefore, this does not seem to suit the cloud environment in which there are always "mass, repeated and structural" transfer of personal data within and outside the EU.

It is clear that in the GDPR, consent is not intended to be the main option for legitimising international data transfer in cloud computing.

2.3.3.2.2 Expanding the Scope of Standard Contractual Clauses

The GDPR continues to allow for international transfer of personal data which is based on SCCs approved by the Commission under Article 26(2) of the DPD, but it significantly states that such data transfers can be made without requiring any specific authorisation from a DPA, whereas prior to the GDPR, many Member States required notification of the data transfer and/or authorisation from the relevant DPA before the data transfer could proceed.[217] Existing SCCs which were implemented under the DPD remain valid.

Apart from that, the GDPR introduces two more types of SCCs to cover more

[214] Eoin Carolan, 'The Continuing Problems with Online Consent under the EU'Emerging Data Protection Principles' (2016) 32 CLS Rev 462, 473.
[215] Schwartz, 'EU Privacy and the Cloud: Consent and Jurisdiction Under the Proposed Regulation'(n129) 2.
[216] GDPR, Rec 111 and 113.
[217] GDPR, Arts 46(2)(c) and 93(2).

scenarios of data transfer. Firstly, it introduces SCCs adopted by individual DPAs and approved by the Commission in Article 46(2)(d). Data transfers which are based on these DPA clauses do not require further authorisation from the DPA. The GDPR does not prevent controllers or processors from including SCCs in a wider contract, such as a contract between the processor and the sub-processor, and adding other clauses or additional safeguards as long as they do not contradict, directly or indirectly, the DPA clauses.[218] This would provide national alternatives to the Commission approved clauses.

Secondly, it introduces SCCs between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation, which is subject to authorisation from the competent DPA for data transfer in Article 46(3)(a) and this must be subject to a consistency mechanism under Article 63.[219]

This mechanism requires DPAs across all Member State to cooperate with each other and, where relevant, with the Commission and if any matter affects more than one Member State, it should be referred to the European Data Protection Board (EDPB) to obtain an opinion.[220] It also allows CSPs to deal with only a competent DPA.[221] Identifying the competent DPA is subject to an one stop shop rule in Article 56.[222] This mechanism would be beneficial to CSPs as it ensure more consistent compliance requirements across the EU.

Since the existing SCCs must be used without modification, all these new clauses would provide more options to be adopted by different kinds of CSPs to transfer personal data outside the EU. They probably cover better various circumstances of the data transfers within the cloud.

2.3.3.2.3 Formally Recognising Binding Corporate Rules

The GDPR provides for the first time official recognition to BCRs for controllers and

[218] GDPR, Rec 109.
[219] GDPR, Art 46(4).
[220] GDPR, Arts 63 and 64(2).
[221] GDPR, Arts 64(1).
[222] The competent DPA is the DPA of the Member State where the main establishment is located.

processors as a legal basis for "adducing appropriate safeguards" for data transfer in Article 46. It also provides a definition of them in Article 4 (20) as

> personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity

The requirements for BCRs under the GDPR are partially in line with the recommendations that were previously issued by the A29WP, but there are some material differences as follows:

(1) BCRs are no longer available only to a corporate group but also to 'a group of undertakings, or a group of enterprises engaged in a joint economic activity, including their employee', which is not part of the same corporate group.[223] However, the GDPR leaves several practical questions open, for instance what criteria will be used to define whether companies are engaged in a joint economic activity? which rules for determining a lead DPA will be used in cases of joint economic activity?[224] Accordingly, whether sub-CSPs will be part of a group of enterprises engaged in a joint economic activity remains in question.

If sub-CSPs and sub-sub-CSPs, who engage in the same set of personal data processing qualify as part of such a group, this would reflect the business reality of cloud computing where CSPs often sub-contract with other CSPs supplying them with PaaS or IaaS for providing their own service to the users. BCRs under the GDPR will be very positive and useful to CSPs since it provides them a more convenient way to ensure compliance with the EU DP law.

(2) BCRs need to be approved by a competent DPA and, once such approval is obtained, each transfer of personal data made under the BCRs does not require any

[223] GDPR, Rec 110 and Art 47(1).
[224] Wanne Pemmelaar, Anna Van Der Leeuw-Veiksha and Charlotte Mullarkey, *BCRs under the GDPR: Practical Considerations* (PL&B UK Reports, March 2017) 7.

further approval.[225] The approval process of BCRs is subject to the "consistency mechanism" which is a new concept introduced by the GDPR.[226] This mechanism allows an organisation to coordinate with only the competent DPA for its BCRs.[227] Compared to the previous applicable system in which even if BCRs are approved by the competent DPA, BCRs must still be formally authorised by each national DPA in accordance with the applicable national law. This is likely to make the adoption of BCRs easier and to reduce the inconsistencies in the interpretation and the implementation of BCRs from one DPA to another.[228]

(3) The GDPR explicitly sets out a minimum requirement for BCRs, without specifically mentioning controllers or processors in Article 47(2). These requirements are partially in line with the recommendations previously issued by the A29WP, with some differences as follows:

(a) the obligation to comply with general DP principles (e.g. purpose limitation and DP by design and by default);

(b) the rights of the data subjects not to be subject to profiling;

(c) liability for BCR breaches by any non-EU group member;

(d) the tasks of the DP officer to monitor compliance with BCRs;

(e) BCR compliance mechanisms within the company group;

(f) mechanisms for reporting and recording of changes to the BCRs.[229]

Compared to the requirements previously set out by A29WP, which may be interpreted inconsistently from one DPA to another, BCRs under the GDPR would be more streamlined. This would make them a much more attractive option for business and at the same time this is likely to make EU cloud users feel more confident to adopt cloud services from CSPs who implement the BCRs. BCRs might become an option for data transfer in the cloud.

Apart from the minimum requirements under Article 47, there might be more

[225] GDPR, Arts 46(2)(b) and 47.
[226] GDPR, Arts 47(1).
[227] GDPR, Arts 63-67; Identifying the lead DPA is subject to one stop shop rule under Article 56.
[228] Anna Pateraki, 'EU Regulation Binding Corporate Rules Under the GDPR—What Will Change?' (2016) 13 Bloomberg BNA World Data Protection Report 1, 2-3.
[229] GDPR, Arts 47(2)(d)(e)(f)(h)(k)(m).

guidelines and requirements spelled out from other sources, including (1) the Commission may implement Acts to specify the format and procedures for the exchange of information regarding BCRs between controllers, processors and DPAs or (2) EDPB may issue more elaborate BCRs guidelines.[230]

In February 2008, the A29WP has issued two new sets of guidelines on BCRs that reflect the requirement under the GDPR.[231] These guidelines include tables setting out the elements and principles of BCRs for controller and for processor.

2.3.3.2.4 Replacing the EU-US Safe Harbor Agreement with the EU-US Privacy Shield

The GDPR did nothing specifically to resolve the criticisms of the EU-US Safe Harbor Agreement. However, the revelations of the PRISM and TEMPORA scandals in 2013, and the CJEU's decision in *Schrems* , had already lead to the invalidation of Safe Harbor prior to the GDPR coming into operation.[232] Resolution had to be found outside the GDPR.

The Commission adopted on 12 July 2016 its decision that the EU-US Privacy Shield ensured an adequate level of protection under Article 45 of the GDPR.[233] It was designed by the US Department of Commerce (DoC) and the European Commission to provide EU or US companies with a mechanism to comply with EU DP law when transferring personal data from the EU to the US. To join this system, a US-based organisation will be required to self-certify to the DoC and to publicly commit itself to comply with the Framework's requirements. Once an eligible organisation makes a public commitment to comply with the Framework's requirements, the commitment will become enforceable under US law.

[230] GDPR, Arts 47(3), 93(2) and 70(1)(i).
[231] A29WP, Working Document Setting up a Table with the Elements and Principles to be Found in Binding Corporate Rules (Adopted on 28 November 2017, As last Revised and Adopted on 6 February 2018).
[232] See more discussions in chapter 4.
[233] European Parliament, *Commission Implementing Decision of 12.7.2016 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield* (Brussels, 1272016 C(2016) 4176 final).

Most of the principles in the Safe Harbor Framework have been integrated into Privacy Shield Principles. There are improvements that are brought by this shield as follows:

(1) *Stronger obligations on company handling data*

(a) the Privacy Shield notice requirements are more specific and request more detailed information which a company must provide;

(b) there must be regular reviews of participating companies by the DoC as to their compliance with the Privacy Shield Framework;

(c) the company must adhere to the Privacy Shield Principles for as long as it retains the data, even if the self-certification were to be terminated;

(d) the company may only transfer personal data to a third party (onward transfer) for limited and specified purposes and provide at least the same level of protection as is required by the Privacy Shield Principles.

(2) *Clearer limitations and safeguards with respect to U.S. government access*

(a) more transparency regarding the use of the exception to the Privacy Shield principles by US authorities for the purposes of law enforcement or national security;

(b) establishing the possibility of redress in the area of national intelligence for Europeans through the mechanism of an Ombudsperson within the Department of State, who will be independent from the national security services.

(3) *More Effective protection of Europeans' rights*

(a) the EU data subjects have the right to bring complaints directly to independent dispute resolution bodies;

(b) the US DoC has committed itself to resolve complaints about a company's non-compliance with the Privacy Shield Principles;

(c) the EU data subjects may invoke binding arbitration by a "Privacy Shield Panel" composed of at least 20 arbitrators designated by the US DoC and the European Commission.

Concerns were raised regarding the progress of Privacy Shield, just as they had been earlier in relation to Safe Harbor Decision. Again, the self-certification system of

Privacy Shield and the possibility of the collection of massive and indiscriminate data by the US administration, which will be an unjustified interference with the fundamental rights of EU individuals, and the insufficient independence of the Ombudsperson could then lead to doubts as to whether the DP offered under this shield is equivalent to that of the EU.[234]

In September 2016, Digital Right Ireland (DRI) filed a challenge with Europe's second highest court, the Luxembourg-based General Court.[235] DRI has sought an annulment of the Commission's Adequacy Decision which approved and adopted the Privacy Shield. If this case were to be successful, it would invalidate the Commission's Adequacy Decision which approved and adopted the Privacy Shield.

Following that, in October 2016, the Privacy Shield faced another challenge from the French privacy advocacy group La Quadrature du Net, which has been claiming that the Privacy Shield does not provide sufficient protection for personal data that is transferred from the EU to the US.[236] Currently, we still await the decisions of these two cases.

On 25 January 2017, the Privacy Shield faced another big challenge resulting from section 14 of an executive order entitled 'Enhancing Public Safety in the Interior of the United States' signed by US President Trump, which stated that

> Agencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information.[237]

This will probably deepen the current concerns about the robustness of the mechanism

---

[234] A29WP, *Opinion 01/2016 on the EU – U.S. Privacy Shield Draft Adequacy Decision* (16/EN WP 238, Adopted on 13 April 2016); EDPS, *Opinion 4/1026 on the EU-U.S. Privacy Shield Draft Adequacy Decision* (30 May 2016). See more discussion in chapter 4. See generally in Mbioh WR, 'Do The Umbrella Agreement and Privacy Shield Comply with the "Saugmandsgaard Mandatory Requirements"?' (2017) 20 J Internet L 23.
[235] Case T-670/16 Digital Rights Ireland v Commission, action brought on 16 September 2016.
[236] Case T-738/16 La Quadrature du Net and Others v Commission, action brought on 30 October 2016.
[237] The White House, 'Executive Order: Enhancing Public Safety in the Interior of the United States' (*25 January 2017*) <https://www.whitehouse.gov/the-press-office/2017/01/25/presidential-executive-order-enhancing-public-safety-interior-united> accessed 1 March 2017.

for EU-US data transfer. Although the Commission still does not have any responses to the implications of Trump's executive order at present, the Privacy Shield is very likely to be suspended by the Commission if an adequate level of protection for EU citizens' personal data under U.S. law can no longer be guaranteed. In April 2018, the Irish high court also included the questions on the validity of Privacy Shield in the case delivered to the CJEU for ruling on the validity of the SCCs.[238] As a result, whether this shield could be used to ensure an adequate level of DP, as provided by the EU DP law to EU cloud users when their personal data have been transferred to the US, remains uncertain.

2.3.4 Conclusions

The data export rule of the DPD failed to protect the DP rights of the EU data subjects when their data have been transferred outside the EU into the cloud. As far as trust in the cloud is concerned, the data export rule under the GDPR is more helpful because it extends the rule to cover an "onward transfer" of data from the non-EU country to another non-EU country, but how EU data subjects can enforce their rights against such non-EU data importers and data exporters is left in question.

The GPDR does make an effort to restrain the use of standard form of consents given by data subjects as the main way to legitimise data exports. This recognises the difficulties in obtaining meaningful consent from the data subject. Consent will not be allowed to use for a massive and repetitive transfer of personal data, so will largely no longer be an option for data transfer within the cloud. Kosta suggests that if the role of consent is reduced, developing of efficient and clear provisions for handling data under the concept of "suitable safeguards", regardless of the legal basis of the data transfer, will be one possible solution for this problem.[239]

The GDPR deals with the inflexibility of the current SCCs approved by the Commission by introducing two more types of such clauses, including DPA clauses (Article 46(2)(d)) and ad-hoc clauses (Article 46(3)(a)). This would benefit non-EU

[238] See section 2.3.3.2.4.
[239] Kosta, *Consent in European Data Protection Law* (n157) 318; Gabriela Zanfir, 'Forgetting About Consent. Why the Focus Should be on "Suitable Safeguards" in Data Protection Law' in Serge Gutwirth, Ronald Leenes and Paul De Hart (eds), *Reloading the Data: Multidisciplinary Insights and Contemporary Challenges* (Springer 2013).

CSPs to provide their services to EU data subjects, but the question remains who will be a DPA in non-EU country to approve ad-hoc clauses and corporate with other DPA in the Member State under the consistency mechanism.

BCRs under GDPR do seem to be a useful option for data transfer within a multinational group of companies but in the cloud this may often not be the case. The consistency mechanism which BCRs are subject to could ensure that CSPs would face more consistent compliance requirements across the EU and could reduce the cost and time for the approval process because CSPs are allowed to be subject to the lead DPA.

The GDPR introduces a one stop shop rule for identifying the lead DPA who monitor each data processing, which would fix the problem of being responsible to multiple DPA in different countries and then could reduce administrative burdens and inconsistencies which currently exist for CSPs who operate across multiple EU Member States under the DPD.[240] However, it may raise difficulties for the lead DPA to exercise its role effectively outside its own jurisdiction and for data subjects in seeking to enforce their rights outside their own jurisdiction.[241]

Since the SCCs and Privacy Shield are currently under challenge, and the role of consent has been heavily restricted in the GDPR, it remains to be seen what will be left as a valid legal basis for CSPs for transferring data outside the EU. The lack of an effective and practical mechanism used for safeguarding the DP rights of EU data subjects for international data transfer, would make EU data subject hesitate to entrust their data with CSPs. Non-EU CSPs might want to leave EU market to avoid being subject to the liability for the non-compliance with the GDPR.

As a result, adopting an other kind of approach might be helpful for ensuring the DP.[242] A potential way for EU cloud users is probably to encrypt their data before uploading them into the cloud and a way for CSPs who want to deliver their services to

[240] W. Gregory Voss, 'Looking at European Union Data Protection Law Reform through a Different Prism: the Proposed EU General Data Protection Regulation Two Years Later' (2014) 17 J Internet L 11, 13; Commission, 'Data Protection Day 2014: Full Speed on EU Data Protection Reform' (Brussels, 27 January 2014) <http://europa.eu/rapid/press-release_MEMO-14-60_en.htm> accessed 1 May 2018.
[241] See generally in Paolo Balboni, Enrico Pelino and Lucio Scudiero, 'Rethinking the One-Stop-Shop Mechanism: Legal Certainty and Legitimate Expectation' 30 CLSR Rev 392.
[242] See more details in Chapter 5.

EU cloud users might be to make it clear in the contract where the data will be stored or processed and what is the mechanism they will use to ensure a high level of DP regarding the EU DP law.

CONCLUSIONS

The intrinsic complexity of cloud computing in terms of its actors creates difficulties about identifying controllers, processors and sub-processors; the difficulties of cloud processing operating across local borders creates enormous difficulties in pinning down when EU law applies and what Member State law in particular. Political issues around export of data to non- EU countries, and in particular the revelations about the US state agency access to data in the US- controlled have crated as furore of doubt and anger and have led to legal reform in both the GDPR and the Privacy Shield.

The legal problems discussed in this chapter have provided a number of risks and uncertainties to the DP rights of EU data subject. This situation is likely to affect the three key factors for creating trust in cloud computing, identified in chapter 2: (1) *transparency and control* – these problems bring about a lot of legal uncertainties regarding how their data will be collected or processed, by whom and for what purposes and whether their data will be protected at the level required by the EU DP law, and this can make cloud users feel that they will lose control over their data; (2) *accountability* – these problems create barriers that prevent CSPs from being responsible enough to comply with the obligations imposed by the EU DP law and to be liable to provide cloud users with remedies for any damages resulting from their actions; and (3) *data security* – these problems give rise to a variety of risks to the security of data residing in the cloud.

Accordingly, the DP problems could potentially weaken user trust in cloud computing, then reducing its uptake and usefulness. Although the GDPR has tried to address some of these problems, some seem intractable, particularly the more political problems. In the next chapter the problems relating to intelligence service access to data in the cloud are considered in more detail.

CHAPTER 4

LEGAL PROBLEMS REGARDING THE EU AND US LEGAL FRAMEWORKS GOVERNING ACCESS TO PERSONAL DATA HELD IN CLOUD COMPUTING BY LAW ENFORCEMENT AND NATIONAL INTELLIGENCE AGENCIES

INTRODUCTION

While cloud computing is a major driver for economic development, cloud services can also be used for crimes and acts of terrorism, particularly when used to store and communicate data used for these purposes in secret and with anonymity. This is why the use of cloud computing has received attention from law enforcement agencies (LEAs) and national intelligence agencies (NIAs). These agencies may feel the need to gain access to and/or use the data residing in the cloud, for the sake of preventing or tackling these crimes and acts of terrorism. This may involve seeking access to storage and services provided by private sector cloud service providers (CSPs) creating dilemmas relating to the privacy and confidentiality of ordinary users. It is one of the arguments of this thesis as discussed in chapters 2 and 3 that such covert permission of surveillance if insufficiently targeted to those under suspicion and without appropriate safeguards of transparency and redress, may badly affect the trust users place in cloud services, which then affect their uptake.

It should be noted that there are differences between the roles taken by LEAs (e.g. the police in the United Kingdom (UK)) and by NIAs (government agencies: e.g. the government communication headquarters (GCHQ), MI5 in the UK and the Central Intelligence Agency (CIA), the National Security Agency (NSA) in the United Sates (US)).[1] However, drawing distinctions between their activities in the context of law

[1] GCHG is responsible for defending the Government from cyber threats, providing support to the Armed Forces and striving to keep the public safe, in real life and online. See< https://www.gchq.gov.uk/who-we-are> accessed 1 April 2018; MI5, as defined in the Security Service Act 1989, is responsible for protecting national security against threats such as terrorism, espionage and sabotage, the activities of agents of foreign powers and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means. See < https://www.mi5.gov.uk> accessed 1 April 2018; The CIA is the main intelligence agency in the US which is responsible for all intelligence matters related to national

enforcement and national security is not always an easy task.[2] Some agencies, such as the Federal Bureau of Investigation (FBI), which is a federal LEA and NIA in the US, have both law enforcement and intelligence responsibilities.[3] This chapter focuses on the activities of both the LEAs and NIAs of the US as public agencies, which may lead to the violation of the privacy rights of the EU cloud users.

The purpose of this chapter is to address Research Question E: what are the legal problems affecting trust in cloud computing that arose out of the Snowden revelations about covert state surveillance of cloud users? The Snowden revelations in 2013 are discussed below to demonstrate:

(1) How the activities of LEAs and NIAs of one country may infringe the privacy standards of other countries which the data subjects of those countries expect to be upheld;

(2) How such breaches could potentially affect trust between these countries;

(3) How the law can seek to protect the privacy rights of foreign users, especially in cases of apparent abusive data access by foreign public agencies and;

(4) What should be the approach for rebuilding trust in such situations where it is damaged (discussed further in chapter 5).

The reasons for focusing on the activities of US LEAs and NIAs in relation to EU cloud users are because

(1) almost all major CSPs are headquartered in the US (e.g. Google, Amazon and Yahoo);

(2) the US government is thus the State with the most potential power to infringe EU privacy standards;

---

security, including human intelligence, direct insertion and operations inside nations; The CIA is under the Department of Defense. See <https://www.cia.gov/index.html > accessed 1 April 2018; The NSA is responsible for collecting, monitoring, and processing information and data for counterintelligence and foreign intelligence actions, specializing in signals intelligence (SIGNIT), hacking, anti-hacking and cryptological efforts. The NSA is under the Department of Defense. See <https://www.nsa.gov/about/mission-strategy/> accessed 1 April 2018.

[2] Cristina Blasi Casagran, *Global Data Protection in the Field of Law Enforcement: An EU Perspective* (Routledge 2016) 169-171; CoE, *Criminal Justice Access to Data in the Cloud: Challenges: Discussion Paper Prepared by the T-CY Cloud Evidence Group* (26 May 2015, Strasbourg, France, T-CY (2015)10) 6.

[3] See <https://www.fbi.gov > accessed 1 April 2018.

(3) the EU and US have very different approaches towards privacy protection;

(4) extensive use of US owned cloud services by commercial users means such activities might seriously affect trust of EU data subjects in cloud computing generally.

There are two main sections in this chapter. After this introduction, section one will consider the legal frameworks regarding access to personal data held in cloud computing for preserving to privacy rights of data subjects in the context of law enforcement and national security. This section is separated into four main sub-sections.

(1) what international multilateral or bilateral legal frameworks protect data subjects against interference with their privacy and private data by the State;

(2) what level of privacy protection EU legal frameworks provide to EU data subjects regarding processing of personal data by LEAs and NIAs. These first two sub-sections aim to show the expectations of legal protection for privacy EU data subjects have and which they expect to be upheld when they entrust their personal data to foreign CSPs.

(3) what level of privacy protection US legal frameworks give to US and, importantly, to EU data subjects, especially when US LEAs and NIAs seek access to personal data stored with US CSPs or in US located data centres ("US-controlled cloud").

(4) what level of privacy protection the EU-US agreement provides to EU data subjects when personal data has been transferred from the EU to the US.

Section two is divided into three sections. The first section explores defects in US legal instruments that lead to mass surveillance by LEAs and NIAs. The second section discusses whether US legal frameworks, and EU-US instruments for data transfer from the EU, which were in operation up to the Snowden revelations and the subsequent *Schrems* case, offered EU cloud users sufficient privacy protection to meet their expectations – and if not, why not. This analysis is crucial because these problems seem to affect, as has been shown in chapter 2 and 3, the trust of EU users in cloud computing. In particular, the Snowden revelations in 2013 are introduced and analysed as a landmark case study, which raised concerns in the EU about the privacy protection in the

cloud. Subsequent events such as the revelations of alleged Russian manipulation of political material on sites like Facebook have also depreciated trust of EU users in cloud services, but they have not had the same systematic impact as most commonly-used cloud services are not actually run by Russia. The third section provides an analysis of whether the legal frameworks proposed *subsequent to* the Snowden revelations by the US and EU work satisfactorily to address the existing problems, and leads into the discussion in the next chapter on what possible approaches exist both in law and beyond law to improve user trust in the cloud.

Lastly, conclusions are drawn from the chapter as a whole.

1. LEGAL FRAMEWORKS RELATING TO PRIVACY RIGHTS IN THE CONTEXT OF LAW ENFORCEMENT AND NATIONAL SECURITY

1.1 International Multinational/Bilateral Legal Frameworks

1.1.1 European Convention on Human Rights (ECHR)

Article 8 of the ECHR is an international provision regarding privacy rights in the context of law enforcement and national security.[4] It was adopted by the Council of Europe (CoE) in 1950, and then entered into force in 1953. All 28 EU Member States have an obligation to act in accordance with the provisions of ECHR. This Article is interpreted and enforced by the European Court of Human Rights (ECtHR) in Strasbourg.

1.1.1.1 Scope of Article 8

Article 8(1) guarantees that 'Everyone has the right to respect for his private and family life, his home and his correspondence'

The scope of Article 8 has been explored in many cases by the ECtHR. Although, the court's decisions are not binding, they shed valuable light on how the right to privacy is applied in practice.[5] The notion of "private life" is a broad term encompassing

[4] The Convention for the Protection of Human Rights and Fundamental Freedom, Rome 1950 (European Convention on Human Rights, as amended), 1 June 2010.
[5] See generally in Helen Keller and Stone Alec Sweet, 'The Reception of the ECHR in National Legal Orders' in Helen Keller and Stone Alec Sweet (eds), A Europe of Rights: The Impact of the ECHR on

the sphere of personal autonomy within which everyone can freely pursue the fulfillment of his or her personality and develop his or her relationships with other persons, e.g. health and medical care, death and dying, honour and reputation.[6] The concept of "family life" is not confined solely to marriage-based relationships, but also encompass other *de facto* "family ties" where sufficient constancy is present, such as between same sex couples, siblings and between a single father and his adopted son.[7] The notion "home" is defined with respect to factual circumstances, in particular the existence of sufficient, continuous links with a given location.[8] Both traditional messages and electronic mail in the context of business and professional relationships fall under "correspondence" in Article 8(1).[9]

1.1.1.2 Limitations of Article 8

Article 8(1) is not an absolute right. Article 8(2) provides that public agencies may interfere with the exercise of this right if this is

(a) "In Accordance with the Law"

The interference must be authorised by a rule that is recognised in the national legal order, which covers written law and unwritten law (as interpreted and applied by the courts).[10] Moreover, the laws must be accessible to the citizens and must be formulated with sufficient precision to enable them, if need be with appropriate advice, to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail.[11] In *Malone v UK*, the court considered in 1984 whether the power to intercept telephone conversations had any legal basis. At the time, telephone-tapping

---

National Legal Systems (OUP 2008) ; William Schabas, The European Convention on Human Rights : A Commentary (OUP 2015) 390.

[6] Niemietz v. Germany, no.13710/88, 16 December 1992; Nada v. Switzerland [GC], no. 10593/08, 12 September 2012; Bensaid v. UK, no. 44599/98, 9 February 2001; Hass v. Switzerland, no. 31322/07, 20 January 2011.

[7] Schalk and Kopf v Austria, no. 30141/04, 22 November 2010; Moustaquim v. Belgium, 18 February 1991; Negrepontis-Giannissis v. Greece, no. 56759/08, 3 May 2011; Kroon and Others v. the Netherlands, 27 October 1994; Kruskovic v. Croatia, no. 46185/08, 21 June 2011.

[8] Hartung v. Germany, no. 10231/07, 3 November 2009.

[9] Dumitru Popescu v. Romania(no.2), no. 71525/01, 26 April 2007; Bykov v. Russia [GC], no 4378/02, 10 March 2009; Kennedy v. UK, no. 26839/05, 18 May 2010.

[10] Leyla Sahin v. Turkey [GC], no. 44774/98, 10 November 2005; Sanoma Uitgevers B.V. v. the Netherlands [GC], no. 38224/03, 14 September 2010.

[11] Andersson v. Sweden, no. 12963/87, 25 February 1992, para. 75.

was regulated by administrative practice, the details of which were not published, and without specific statutory authorisation. The court said that there was not sufficient clarity about the scope or the manner in which the discretion of the authorities to listen secretly to telephone conversations was exercised: because this was an administrative practice, it could be changed at any time and this constituted a violation of Article 8.[12]

(b) "Necessary in a Democratic Society"

In 1976, the ECtHR explained in *Handyside v. UK* the meaning of "necessary", that 'it is not synonymous with "indispensable" … neither has it the flexibility of such expressions as "admissible", "ordinary", "useful", "reasonable" or "desirable"'.[13] *Dudgeon v.UK* took the view in 1981 that the Convention was designed to maintain and promote the ideals and values of a democratic society.[14] In summary, what is "necessary in a democratic society" is determined by reference to the balance achieved between the rights of individual and public interest, through the application of principle of proportionality.[15]

(c) "Proportionality"

Proportionality is an important principle in finding a balance between the interests of the individual and the interests of the community, even though this is not explicitly stated in the ECHR.[16] Deciding whether the interference is proportionate to the aim that it pursues, involves consideration of

(1) the interest to be protected from interference;

(2) the severity of the interference;

(3) the pressing social need which the State is aiming to protect.[17]

In *Peck v UK*, it was held in 2003 that the disclosures by the Council of the CCTV material in CCTV News and to the Yellow Advertiser, Anglia Television and the BBC had not been accompanied by sufficient safeguards and, therefore, it constituted a

[12] Malone v. UK, no. 8691/79, 2 August 1984, para 67.
[13] Handyside v.UK, no. 5493/72, 7 December 1976.
[14] Dudgeon v. UK, no. 7525/76, 22 October 1981, para. 53.
[15] Keegan v. Ireland, no. 16969/90, 26 May 1994; Ursula Kilkelly, *A Guide to the Implementation of Article 8 of the European Convention on Human Rights* (Directorate General of Human Rights Council of Europe, Human Rights Handbooks, No 1, 2001) 31.
[16] See Generally in Nick M. Taylor, *Policing, Privacy and Proportionality* (EHRLR, Special Issue, 2003).
[17] Olsson v. Sweden (no.1), no.19465/83, 24 March 1988.

disproportionate and unjustified interference with the applicant's private life and was in breach of Article 8.[18]

(d) "Margin of Appreciation"

The court affords to the State a margin of appreciation when deciding whether an interference with an Article 8 is justified under Article 8(2). The margin of appreciation can be defined as 'the measure of discretion allowed the Member States in the manner in which they implement the Convention's standards, taking into account their own particular national circumstances and conditions'.[19] The ECtHR adopted in 1976 this principle in the *Handyside v. UK*, when it was concerned with whether a decision by the UK government to convict a person for obscene publication, could be classified as 'necessary in a democratic society….for the protection of morals'.[20] The court took the view that in areas as sensitive as morality or religion there was no consensus among States, and that the domestic authorities were better situated to appreciate the social circumstances and to decide how to manage conflictive situations; however, according to the ECtHR itself, this margin is limited, is subject to supervision and will vary as a function of the sensitivity of the issue.[21]

1.1.2 Council of Europe Convention 108

The Convention 108 of the CoE is the first internationally legally binding instrument that grants privacy protection against abuse to individuals regarding the processing of personal data. It entered into force on 1 October 1985 and it is currently ratified by 50 Member States, including 28 EU Member States but does not include the US.[22]

---

[18] Peck v. UK, no. 44647/81, 28 January 2003, section 3.
[19] Yataka Arai-Takahashi, *The Margin of Appreciation Doctrine and the Principle of Proportionality in the Jurisprudence of the ECHR* (Intersentia Publishers 2002) 1; Howard C. Yourow, *The Margin of Appreciation in the Dynamics of European Human Rights Jurisprudence* (Martinus Nijhoff Publishers 1996) 15.
[20] Handyside v.UK, no. 5493/72, 7 December. 1976, paras. 48- 49.
[21] ibid.
[22] The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No. 108, Strasbourg, 28/01/1981.See the list of 50 Member States <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=ylGwf6on > accessed 1 April 2018.
Moreover, in 2001, this Convention was supplemented by an Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data regarding Supervisory Authorities and Trans-Border Data Flows (CETS No181; 8/11/2001).

It set out general DP principles which apply to data processing carried out by both private and public (only by LEAs, not NIAs) sectors. Therefore, personal data held in the cloud must be collected or stored by LEAs only for specific purposes, e.g. for the prevention of a real danger, and should be used exclusively for such purposes.[23] The transfer or communication of personal data should be based on a legitimate interest in sharing the information.[24] The cross-border transfer or communication of the data between Member States is possible, but it should be restricted to and be based on special legal provisions, possibly Mutual Legal Assistance Treaties (MLATs), unless it is necessary for the prevention of serious and imminent danger.[25]

This Convention has been under the process of modernisation since 2010.[26] The new rules will establish a high and uniform level of DP legislation, no matter where their data are stored or processed within the EU and will be compatible with the new EU DP laws, which came into force in May 2018. The significant improvements are for example imposing stronger consent requirements, and direct obligations on the processor and requiring the controller to be able to demonstrate his compliance with the Convention. The CoE published a Draft Modernised Convention 108 on September 2016.[27] The Protocol amending this Convention was adopted on 18 May 2018 and was opened for signature on 10 October 2018.[28]

1.1.3 Budapest Convention on Cybercrime

The Convention on Cybercrime is an international legal instrument which was adopted

[23] Convention 108, Art 5b. Recommendation No R (87) 15 Principle 2.1 and 4.
[24] Convention 108, Art 12. Recommendation No R (87) 15 Principle 5.
[25] Convention 108, Arts 13-15. Recommendation No R (87) 15 Principle 5.
[26] Council of Europe Response to Privacy Challenges and Modernisation of Convention 108, position paper distributed at the 32nd International Conference of Data Protection and Privacy Commissioners, 27-29 October 2010, Jerusalem, Israel. See <http://www.coe.int/en/web/data-protection/modernisation-convention108 > accessed 1 April 2018.
[27] Consolidated text of the modernisation proposals of Convention 108 finalised by the CAHDATA (meeting of 15-16 June 2016 (Draft Modernised Convention 108). See <https://rm.coe.int/16806a616c> accessed 1 April 2018.
[28] Ad hoc Committee on Data Protection (CAHDATA), Protocol (CETS No. 223) amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) CM(2018)2- final, 18 May 2018. See <https://rm.coe.int/16808ac918> accessed 1 July 2018.

by the CoE, with 50 signatories.[29] The US signed this Convention on 23 November 2001, then it entered into force in the US on 1 January 2007. This Convention set out rules for international cooperation between countries in investigating and prosecuting crimes committed against or by means of electronic networks, e.g. computer-related fraud and violations of network security.

When US LEAs investigating a crime believe that electronic evidence is stored by CSPs on servers located abroad, such LEAs will be allowed to obtain access to the data held in the cloud in two different situations.

(1) Article 31 – LEAs of one Member State can make a request to another Member State to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Member State. And this request will be responded on an expedited basis, e.g. there are grounds to believe that relevant data is particularly vulnerable to loss or modification.

(2) Article 32 – Two types of transborder access to data, without consent of another county, are allowed. Firstly, LEAs can gain access to publicly available stored computer data, regardless of where the data is located geographically.[30] Secondly, LEAs of one Member State can access or receive, through a computer system in its territory, stored computer data located in another Member State, if such agency obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data through that computer system.[31]

1.1.4 Mutual Legal Assistance Treaties (MLATs)

The MLATs, unlike the multilateral treaties above, are agreements between two or more countries and are the traditional approach to gather and exchange information from foreign agencies or police forces where such information has no other cooperation mechanism in place and is not voluntarily supplied. MLATs are even used to obtain evidence located in one country to assist the investigation or prosecution of transnational

[29] The Convention on Cybercrime, CETS. 185, Budapest, 23 November 2001, Treaty Series No. 18 (2012). See the list of 50 signatories at < https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=tdJwkOmM > accessed 17 November 2016.
[30] Convention on Cybercrime, Art 32(a).
[31] Convention on Cybercrime, Art 32(b).

crime and terrorism in another. Requests are made by a formal international Letter of Request (LOR).

The agreements on mutual legal assistance (MLA) and extradition between the EU and US came into force on 1 February 2010, to strengthen cooperation in criminal matters between EU member States and US authorities in the fight against terrorism and transnational crime.[32] The assistance that can be provided through MLATs traditionally includes: the provision of documents; search and seizure; restraint and confiscation of the proceeds of crime; the provision of telephone intercepted material; and the facilitation of the taking of evidence from witnesses. Therefore, public agencies of both the US and all EU Member States are entitled to make a request to each other to obtain access to data stored on servers of CSPs physically located in or subject to the jurisdiction of foreign territories; however, this request may be refused in exceptional cases, e.g. for public interest or privacy interests.[33]

1.2 EU Legal Frameworks

1.2.1 Council Framework Decision 2008/977/JHA (Framework Decision)

The EU cooperation against terrorism and cross-border crimes with non-EU countries and international organisations became an EU priority with the Treaty of Maastricht in 1993, formally known as the Treaty of European Union (TEU), which set out rules on Justice and Home Affairs (JHA), as the EU's third pillar.[34] The idea of an Area of Freedom, Security and Justice (AFSJ) was introduced in May 1999, in the Amsterdam Treaty.[35] The term JHA later was renamed "Police and Judicial Co-operation in Criminal Matters" (PJCCM) to reflect its reduced scope.

---

[32] Mutual Legal Assistance; Agreement Between the United States of America and the European Union, Signed at Washington June 25, 2003.
[33] Council of the Europena Union, *Handbook on the Practical Application of the EU-U.S. Mutual Legal Assistance and Extradition Agreements* (Brussels, 25 March 2011, 8024/11).
[34] The TEU was signed in Maastricht, 7 February 1992, and entered into force on 1 November 1993. The Maastricht Treaty introduced the three pillar structure of the EU on 1 November 1992, including (1) European Community; (2) Common Foreign and Security Policy; (3) Police and Judicial Co-operation in Criminal Matters.
[35] Treaty of Amsterdam Amending the Treaty on European Union, the Treaties Establishing the European Communities and Certain Related Acts, 2 October 1997, Art 1(5).

The Framework Decision, replaced subsequently by the Police and Criminal Justice Data Protection Directive, was the first step towards a horizontal legal framework setting up a standard for privacy protection regarding the processing of personal data between competent authorities (LEAs), while guaranteeing a high level of public safety.[36] It relied heavily on the principles and definitions which were provided in Convention 108 and the Directive 95/46/EC. Regarding principles of lawfulness, proportionality and purpose, personal data must be collected only for specified, explicit and legitimate purposes and must be processed only for the same purpose for which data were collected.[37] Processing of the data shall be lawful and adequate, relevant and not excessive in relation to the purposes for which they are collected.[38] The transfer of personal data to competent authorities in third countries or to international organisations was allowed under certain circumstances, e.g. for investigation of criminal offenses or for execution of criminal penalties.[39]

1.2.2 EU Charter of Fundamental Rights (EU Charter)

The significant change of the EU's power to adopt measure for PJCCM was made by the Lisbon Treaty, which entered into force on 1 December 2009. This Treaty abolished the old three pillar structure, so that matters which were previously dealt with under the third pillar, will be treated under the same rule as those of the single market (first pillar).[40] The Lisbon Treaty also created an explicit legal basis for regulation of national criminal law in Article 83(1) of TFEU, which enables the EU to establish minimum rules concerning the definition of criminal offences and sanctions in the areas of particularly serious crime with a cross-border dimension to combat them on a common

---

[36] Council Framework Decision 2008/977/JHA of 27 November 2008 on the Protection of Personal Data Processed in the Framework of Police and Judicial Cooperation in Criminal Matters, OJ 2008 L 350/60, 30.12.2008, Art 1(1); Art 2(h) defined "competent authorities" as

> Agencies or bodies established by legal acts adopted by the Council pursuant to Title VI of the Treaty on European Union, as well as police, customs, judicial and other competent authorities of the Member States that are authorised by national law to process personal data within the scope of this Framework Decision.

See more details about the Police and Criminal Justice Data Protection Directive in section 1.2.3.

[37] Framework Decision, Art 3(1).

[38] Framework Decision, Art 3(1).

[39] Framework Decision, Art 13.

[40] Rosemary Jay, *Data Protection Law and Practice* (4th edn, Sweet & Maxwell 2012) chapter 1.

basis.

The entry into force of the Lisbon Treaty makes the EU Charter become legally binding not only for EU institutions and bodies, but also for Member States when they are implementing EU law.[41] Articles 7 and 8 of the Charter, which expressly recognise two fundamental rights relating to not just privacy but DP, are two primary sources of privacy protection in the EU and are also applicable to the PJCCM.

> Article 7:
> Everyone has the right to respect for his or her private and family life, home and communications.
>
> Article 8:
> (1) Everyone has the right to the protection of personal data concerning him or her.
> (2) Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
> (3) Compliance with these rules shall be subject to control by an independent authority.

1.2.3 Police and Criminal Justice Data Protection Directive (PCJDPD)

As mentioned in chapter 3, section 1.2, the EU DP law was modernised to provide a comprehensive approach for protecting the privacy of data subject and to facilitate the free movement of personal data with regard to the personal data processing in private and public (only LEAs, not NIAs) sectors. The Commission originally aimed to set out a single instrument for general DP principles which could apply to the personal data processing in both private and public sectors.[42] But this is not an easy task, it ended up by proposing in 2012 a reform package, including two specific legal instruments, which

[41] The Charter of Fundamental Rights of the European Union, OJ C326/391; 26 October 2012.
[42] PCJDPD, Art 1(1).

are (1) the General Data Protection Directive (GDPR); and (2) the PCJDPD.[43]

The PCJDPD, replacing the Framework Decision, entered into force on 5 May 2016 and is applicable from 6 May 2018.[44] Like the Framework Decision, the activities of agencies dealing with national security issues fall outside the scope of this Directive.[45] It introduces a range of rules to ensure a strong protection to the personal data of EU data subjects involved in criminal proceedings, be it as witnesses, victims, or suspects, regarding the processing of personal data by the competent authority. It extends the scope to cover all data processing, including cross-border and national data processing by competent authorities.[46]

Most of its principles are similar to the GDPR. It requires the controller to be responsible for and be able to demonstrate compliance with the Directive.[47] It also imposes specific obligations on the processor, e.g. not to engage another processor without prior specific or general written authorisation by the controller.[48] In the case of data transfer to third countries, it requires that the transfer must be necessary for the processing purposes of the Directive and can only take place on the basis of e.g. an adequacy decision or where certain situations are met (e.g. protecting vital interests of data subjects).[49] It also provides the data subjects with the right to an effective judicial remedy against a controller or a processor.[50]

Unlike the GDPR, the consent of the data subjects is not a legal ground for processing personal data by competent authorities under this Directive and there is only one ground for lawful data processing under this Directive, which is necessity for the performance of a task carried out by a competent authority for law enforcement

[43] See chapter 3, section 1.2.
[44] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA L 119/89, 4.5.2016.
[45] PCJDPD, Rec 14 and Art 2(3).
[46] PCJDPD, Arts 1 and 2(1).
[47] PCJDPD, Arts 4, 8 and 9.
[48] PCJDPD, Art 22(1).
[49] PCJDPD, Arts 35-39.
[50] PCJDPD, Art 54.

purposes.[51] The rights of the data subject to access information provided by this Directive are quite limited in comparison to those provided by the GDPR, e.g. information regarding data recipients and the period for which the personal data will be stored will be provided to the data subject only in "specific cases".[52]

1.2.4 Privacy and Electronic Communications Laws

In 2002, the Privacy and Electronic Communications Directive (E-Privacy Directive) was passed to preserve the confidentiality of communications and deal with traffic data, spam and cookies.[53] It translated DP principles in the DPD into specific rules only for the telecommunications sector.[54] Providers of a publicly available electronic communication service were obliged to ensure compliance with obligations relating to the secrecy of communications and personal DP, rights and obligations with regard to electronic communications networks and services.

This Directive did not apply to activities concerning public security, defence, state security and the enforcement of criminal law.[55] Article 15(1) allowed Member States to adopt legislative measures to restrict the scope of users' rights under this Directive if such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security, defence, public security, and prevention, investigation, detection and prosecution of criminal offences, or of unauthorised use of electronic communication systems, as referred to in Article 13(1) of Directive 95/46/EC. Article 23 of the current EU DP law, which is the GDPR, also allows Member States to create national data retention provisions authorising the use of data retention schemes.

---

[51] PCJDPD, Art 8 (1).
[52] PCJDPD, Art 13.
[53] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, 31 July 2002. Art 2 (d) of E-Privacy Directive defines "communication" as

> any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information.

[54] E-Privacy Directive, Rec 4.
[55] E-Privacy Directive, Rec 11 and Art 1(3).

However, this Article 15(1) will be replaced by Article 11(2) of the new E-Privacy Regulation whose proposal was published on 10 January 2017 and which is expected to be finalised by the end of 2018.[56] Article 11(2) provides Member States an ability to deviate from the E-Privacy Regulation and pass legislation, such as data retention laws if such a restriction respects the essence of the fundamental rights and freedoms and is a necessary, appropriate and proportionate measure in a democratic society to safeguard one or more of the general public interests referred to in Article 23(1)(a) to (e) of GDPR.

1.2.5 Domestic Laws of EU States

Within the EU, activities conducted by NIAs of 28 EU Member States fall within the sole responsibility of each Member State. Article 4, paragraph 2 of the TEU states that

> the Union shall respect [the Member States] essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security.

This is similar to Article 72 of the TFEU, which stipulates that

> title V of the Treaty pertaining to AFSJ shall not affect the exercise of the responsibilities incumbent upon Member States with regard to the maintenance of law and order and the safeguarding of internal security.

Moreover, article 73 of the TFEU allows the Member States to

> organise between themselves and under their responsibility such forms of cooperation and coordination as they deem appropriate between the [competent national agencies] responsible for safeguarding national security.

As electronic surveillance is a state function, the EU arguably lacks any competence to legislate in this area. Furthermore, the CJEU does not have any jurisdiction over cases

[56] Proposal for a Regulation of the European Parliament and of the Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) COM/2017/010 final - 2017/03 (COD).

that involve surveillance conducted by NIAs in order to safeguard the internal security of several Members States. However, when conducting electronic surveillance in the cloud, either foreign or domestic, the 28 EU countries are subject to the ECHR Article 8 and the EU Charter Article 7 and 8 for preserving the individuals' privacy.[57]

For example, the UK has passed domestic regulations which restrict the power of NIAs to the requirements of ECHR. The Interception of Communications 1985 (ICA) was to provide a clear and comprehensive statutory framework for the interception of communications as a result of the decision of ECtHR in *Malone v UK* that forced the UK government to delineate more precisely, by way of statutory provision, which would allow for the lawful interception of communications and provide a redress mechanism for anyone who wished to complain about that interception.[58] The Regulation of Investigatory Power Act 2000(RIPA) and the Data Retention and Investigatory Power Act 2014(DRIPA), which then were replaced by the Investigatory Power Act 2016, are also regulations restricting the use of the UK NIAs power regarding, e.g. the interception of communications, the carrying out of surveillance and the use of covert human intelligence sources.[59]

Moreover, the UK government has now passed a new DP law, which is the Data Protection Act 2018, to update and strengthen the DP laws so they are fit for the digital age.[60] This Act includes three sets of specific rules for data processing, including rules (1) for general data processing; (2) for law enforcement processing; and (3) for intelligence services processing.[61] This is the first time that data privacy has been regulated for the intelligence services. The data processing for the intelligence services is based on the international standards, which will be provided in the modernised Convention 108 as was mentioned in section 1.1.2.

---

[57] See section 1.1.1 and 1.2.2.
[58] Interception of Communications Act 1985, Chapter 56, 25 July 1985: Malone v. UK, no. 8691/79, 2 August 1984.
[59] Regulation of Investigatory Power Act 2000, Ch 23, 28 July 2000; Data Retention and Investigatory Power Act 2014, Ch 27, 17 July 2014; Investigatory Power Act 2016, Ch 25.
[60] See more details, available at <https://www.gov.uk/government/collections/data-protection-act-2018> accessed 1 July 2018.
[61] UK Data Protection Act 2018
< http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf > 1 July 2018.

Although the UK is leaving the EU, it will have to adhere to the current EU law for about a year as a Member State and, if it wants to continue exchanging data with EU countries, the UK will have to demonstrate its compliance with the principles governing the EU law even after Brexit.[62] As a result, even though this Act is not based on the EU DP laws, it still implements the GDPR standard across all general data processing and implements the PCJDPD standard for law enforcement processing.

1.3 US Legal Frameworks

1.3.1 General Legal Frameworks for Privacy Rights Protection

1.3.1.1 The Fourth Amendment to the US Constitution

The Fourth Amendment does provide a legal basis to provide the protection for US persons against all areas where a person has a reasonable expectation of privacy. (including against intrusion by government).[63] It guarantees that

> [t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[64]

Although, the US Constitution contains no express guarantee of the right to privacy, it does have restrictions on the interference in both physical and virtual spaces deemed to be part of individuals' private sphere.[65]

As can be seen in the landmark decision of *Katz v. United States*, the US Supreme Court concluded that the government's activities in electronically listening to and recording the petitioner's words while using a public phone booth violated "his

---

[62] UK Department for Digital Culture Media & Sport, 'Data Protection Bill Factsheet - Overview' (*11 October 2017*) <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/644634/2017-09-13_Factsheet01_Bill_overview.pdf> accessed 1 November 2017.
[63] The US persons include US citizens and US residences.
[64] The Fourth Amendment of the U.S. Constitution: Searches and Seizures 1791.
[65] See generally in Samuel D. Warren and Louis D. Brandeis, 'The Right to Privacy : the Implicit Made Explicit' (1890) 4 Harv L Rev 193.

expectation of privacy".[66] Therefore, determining whether a particular government action regulated by the Fourth Amendment is subject to whether it infringed, on reasonable expectations of individuals' privacy. In this case, the US Supreme Court found that the Fourth Amendment does not apply to a physical search of a premise overseas, where the person invoking the right was a non-US person.[67] Therefore, the Fourth Amendment does not provide protection to EU persons.

1.3.2 Sectoral Federal Legal Frameworks for Access to Data by Law Enforcement and Nation Intelligence Agencies

1.3.2.1 Privacy Act of 1974

This Act establishes general rules governing the collection, maintenance, use, and dissemination of personal data of US persons by federal government agencies, including LEAs, but excludes NIAs.[68] It applies only to the information contained within a "system of records" i.e. a database described as a

> group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.[69]

This Act in principle prohibits the disclosure of this record unless there is a written consent of the individual to whom the record pertains or the disclosure is pursuant to one of twelve statutory exceptions, such as to the order of a court of competent jurisdiction.[70] It also gives individuals the right to sue agencies for the violations of their rights and to obtain, depending on circumstances, damages or injunctive relief.[71] Agencies may be criminally prosecuted for certain violations of this Act.[72] Moreover, these same provisions afford individuals a judicial remedy for violations of the Privacy Act.

[66] Katz v. United States, 389 US 347, 362, the US Supreme Court, Judgment of 18 December 1967.
[67] US v. Verdugo-Urquides, 494 U.S. 1092, the US Supreme Court, Judgment of 28 February 1990.
[68] The Privacy Act of 1974, Pub. L. 93-579. 88 Stat 1986. 5 U.S.C. § 552a.
[69] 5 U.S.C. § 552a(a)(5).
[70] 5 U.S.C. § 552a(b).
[71] 5 U.S.C. § 552a(g).
[72] 5 U.S.C. § 552a(i).

However, the application of this Act is limited to US persons.[73]

1.3.2.2 Foreign Intelligence Surveillance Act of 1978 (FISA)

This US federal law attempted to provide judicial and congressional oversight of the government's covert surveillance activities (NIAs' activities), while maintaining the secrecy necessary to effectively monitor national security threats.[74] It set out procedures for physical and electronic surveillance of foreign intelligence information and also created the Foreign Intelligence Surveillance Court (FISC) for reviewing the applications relating to electronic surveillance. Conducting electronic surveillance on foreign entities and US persons was allowed under two main circumstances, with and without court order.

The President could under FISA authorise electronic surveillance to acquire foreign intelligence information for periods of up to one year without a FISC court order where the Attorney General (AG) certified in writing under oath that there was 'no substantial likelihood that the surveillance will acquire the contents of any communication to which a US person is a party,' provided the surveillance is directed solely at communications among or between foreign powers, or 'the acquisition of technical intelligence from property or premises under the open and exclusive control of a foreign power'.[75]

Where the government had accidentally intercepted communications 'under circumstances in which a person has a reasonable expectation of privacy and a warrant was required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States,' the government was required to destroy those records, 'unless the Attorney General determines that the contents indicate a threat of death or serious bodily harm to any person'.[76] This Act was amended by the US Patriot Act in 2001, the Protect America Act in 2007, and was finally amended by the Foreign Intelligence Surveillance Amendments Act in 2008.

---

[73] 5 U.S.C. § 552a(a)(2).
[74] The Foreign Intelligence Surveillance Act of 1978, Pub- L. 95-511, 92 Stat.50 U.S.C. § 1801, 25 October 1978.
[75] 50 U.S.C. § 1802.
[76] 50 U.S.C. § 1806.

1.3.2.3 Electronic Communications Privacy Act of 1986(ECPA)/ Stored Communications Act of 1986 (SCA)

The ECPA, which governs activities of both LEAs and NIAs in obtaining access to electronic communications, has three titles which provide different levels of protection depending on the perceived importance of the privacy interest involved. [77] Title I: 18 U.S.C. § 2510 - 2522 (the Wiretap Act) prohibits the intentional, actual or attempted interception, use, disclosure, or procurement of any other person to intercept or endeavor to intercept any real time wire, oral and electronic communications in criminal investigations. But a judge may issue a warrant authorising interception of communications for up to 30 days upon a showing of probable cause that the interception will reveal evidence that an individual is committing, has committed, or is about to commit a "particular offense" listed in 18 U.S.C. § 2516.[78]

Although, this Act does not explicitly state whether it applies to non-US persons, the U.S. Court of Appeals for the Ninth Circuit in case of *Zheng v. Yahoo! Inc.* unanimously affirmed the ruling of a district court that the provisions of the ECPA prohibiting internet service providers from disclosing the contents of stored communications apply whenever the requested documents are stored within the US.[79] Thus, US stored electronic communications of both US and non-US persons are protected by this Act.

Title II :18 U.S.C. § 2701- 2712 (SCA 1986) governs the access to stored content communications stored by an Electronic Communication Service (ECS) or a Remote Computing Service (RCS).[80] It aims to protect the privacy of an individual's electronic communications and provides public agencies with the means for accessing these communications and related records.

---

[77] The Electronic Communications Privacy Act 1986, Pub.L 99-508. 100 Stat. 1848. 18 U.S.C. § 2510-22. This Act has been amended several times i.e. by the Communications Assistance to Law Enforcement Act 1994, the US Patriot Act 2001 and the FISAA 2008.
[78] 18 U.S.C. § 2518(5).
[79] Zheng v. Yahoo Inc.,2009 WL 4430297 at 4, No. C-08-1068 MMC, the US District Court, California, Judgment of 2 December 2009.
[80] The Store Communications Act 1986. Pub.L. 99-508. 100 Stat 1848. 18 U.S.C. § 2701- 2712, 21 October 1986.

The agency must obtain a warrant to compel disclosure of the content of a wire or electronic communication (e.g. an unopened email) stored by an ECS provider (e.g. Yahoo acts as an ECS provider when a user employs Yahoo Mail service to send or receive an e-mail).[81] And the agency may compel disclosure of a wire or electronic communication (e.g. an opened email) stored by an RCS provider in an electronic communication system (e.g. Amazon acts as an RCS provider when a user employs Amazon Cloud Drive to store data remotely for long-term safekeeping) by obtaining a warrant, without notice to subscribers or users; or by obtaining a court order and subpoena, with prior notice from agencies to subscriber or users.[82]

Tile III: 18 U.S.C. § 3121- 3127 deals with pen registers and a trap and trace device. It requires agencies to obtain a court order for the installation and the use of a pen register or a trap and trace device.

1.3.2.4 USA Patriot Act of 2001

This Act, which was enacted in response to the 9/11 attacks, allowed the US agencies to conduct electronic surveillance against more crimes of terror in order to protect civil rights and civil liberties of US persons.[83] This Act made key changes to the FISA 1978 and ECPA 1986.[84] It granted an additional power to the US agencies, with a judicially approved warrant, to gather foreign intelligence information from various sources and remove all of the legal impediments to the sharing of such information among agencies.[85]

Furthermore, agencies may begin investigating through methods such as wiretapping, tracing phone calls, emails, and other forms of communication without needing to show a direct relationship or connection to terrorism.[86] The most controversial provision is Section 215, which permits the bulk collection of telephone metadata, or the mass collection of basic call-log information, from telecommunications

[81] 18 U.S.C. § 2703(a).
[82] 18 U.S.C. § 2703 (a)(b).
[83] The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (The USA Patriot Act), Pub.L 107-56.115 Stat 272, 26 October 2001.
[84] Title II Enhanced Surveillance Procedures of the US Patriot Act 2001.
[85] Patriot Act, section 203 and 215.
[86] Patriot Act, section 201-202.

companies. This Act expired on 1 June 2015 and was restored in modified form of many provisions in this Act by the US Freedom Act in 2015.

1.3.2.5 Foreign Intelligence Surveillance Amendments Act of 2008 (FISAA)

This Act amends FISA Act of 1978 by adding a new title concerning additional procedures for acquiring the communications of certain *persons outside the US* with a view to tackling espionage or international terrorism against the US (Title VII, Section 702 of FISA (50 U.S. Code § 1881a)).[87] The Attorney General (AG) and Director of National Intelligence (DNI) may jointly authorise the US agencies for a period of up to one year from the effective date of authorisation, to target, without warrant, the communication of non-US persons located outside the US for intelligence purposes.[88] And it requires that the targeting should be conducted in a manner consistent with the Fourth Amendment to the Constitution and follow the guidelines which need to be reviewed by the congressional intelligence and judiciary committees and FISA court.[89]

This Act also authorises the AG and DNI to direct, in writing, an electronic communication service provider to immediately provide the government with all information, facilities, and assistance necessary to accomplish an acquisition.[90] The approval of FISA court is only required in the case of targeting of a US person located outside the US when the acquisition of information is conducted inside the US.[91] This Act was scheduled to expire on 31 December 2012, but two days before the expiration, it was extended by the US senate until 31 December 2017.

1.3.3 Snowden and Schrems: Effect on US Legal Frameworks

1.3.3.1 Snowden Revelations

[87] The Foreign Intelligence Surveillance Amendments Act of 2008. Pub.L 110-261. 122 Stat 2436, 10 July 2008.
[88] 50 U.S. Code § 1881a (a)(b).
[89] 50 U.S. Code § 1881a (c)(f).
[90] 50 U.S. Code § 1881a (h).
[91] 50 U.S. Code § 1881b (a).

In 5 June 2013, the Guardian started to publish the leaked materials provided by one of the most extraordinary whistleblowers in history, named Edward Snowden, who formerly worked as a contractor to the CIA and NSA. It was disclosed that since 2007, the US NSA had been conducting a bulk surveillance of telephone and email communications records under a secret programme called "PRISM" directly on the central servers of nine leading U.S. Internet companies, including Yahoo, Google, Facebook, Apple, Microsoft, Skype, Youtube, AoL and Paltalk, in order to collect metadata including the contents of e-mails, live chats, videos, photos, stored data, Voice over Internet Protocol (VoIP), file transfers and connection logs that enabled analysts to track foreign targets, with the assistance of such companies.[92] But then such Internet companies vehemently denied any knowledge of and participation in PRISM and they rejected any allegations about the ability of NSA to directly tap into their users' data.[93]

The leaked documents also showed that the British intelligence agency, GCHQ (the Government Communication Headquarters), secretly gained access to the global telecom cables for the purpose of mass monitoring of sensitive personal data under a surveillance programme called "TEMPORA" and that such data were shared with US NSA through the PRISM programme.[94] Additionally, the PRISM programme has been conducted under close cooperation with their sister agencies in Australia, Canada and New Zealand – collectively known as "Five Eyes".[95]

---

[92] Barton Gellman and Laura Poitras, 'U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program', Washington Post, 6 June 2013 <http://articles.washingtonpost.com/2013-06-06/news/39784046_1_prism-nsa-u-s-servers > accessed 12 September 2017; Luke Harding, *The Snowden Files: The Inside Story of the World's Most Wanted Man* (Guardian Faber Publishing; Main edition (6 Feb. 2014)).

[93] Frederic Lardinois, 'Google, Facebook, Dropbox, Yahoo, Microsoft, Paltalk, AOL And Apple Deny Participation In NSA PRISM Surveillance Program' (*6 June 2013*) <https://techcrunch.com/2013/06/06/google-facebook-apple-deny-participation-in-nsa-prism-program/> accessed 1 May 2017.

[94] 'NSA Prism Program Slides' (*Friday 1 November 2013*) <https://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document> accessed 1 November 2017; Rosalba O'Brien, Kichael Holden and Mark Hosenball, 'British Spy Agency Taps Cables, Shares with U.S. NSA' (*Reuters UK*, 21 June 2013) <http://uk.reuters.com/article/2013/06/21/uk-usa-security-britain-idUKBRE95K10620130621> accessed 1 November 2017.

[95] Gordon Corera, 'Spying Scandal: Will the 'Five Eyes' Club Open Up?' (*29 October 2013*) <http://www.bbc.com/news/world-europe-24715168> accessed 1 April 2017.

Regarding the agency's targeting rules, the NSA's "contact chaining" practices — whereby an analyst collects records on a target's contacts, and their contacts' contacts — can easily cause innocent parties to be caught up in the surveillance programme.[96] This means that PRISM appeared to allow GCHQ to circumvent the formal legal process that is required to obtain access to personal data from Internet companies based outside the UK.[97]

In addition, Snowden revealed that there was a surveillance program jointly operated by GCHQ (UK) and NSA (US) called "MUSCULAR". These agencies secretly intercepted the main communication links of Google and Yahoo through fiber-optic cables that carry their users' data between their worldwide data centers.[98]

All these revelations raised huge concerns about privacy not only of non-US persons, but also US persons, who had understood that by US law such surveillance activities were only meant for the non-US persons.[99] This provoked a variety of responses from foreign governments and leaders.[100] The response in the EU was mostly based on the concept that privacy for the Europeans is a human right, while for Americans, privacy does seem to be liberty, civil right.[101]

The EDPS issued a statement showing its concern about the implications of the PRISM revelations for the privacy and other fundamental rights of EU data subjects.[102] The A29WP requested clarification on (1) whether the PRISM program is only aimed at

---

[96] Edward Jay Epstein, *How America Lost Its Secrets: Edward Snowden, the Man and the Theft* (Knopf Publishing Group 17 Jan 2017).
[97] Owen Bowcott, 'UK-US Surveillance Regime was Unlawful 'For Seven Years'' (*6 February 2015*) <https://www.theguardian.com/uk-news/2015/feb/06/gchq-mass-internet-surveillance-unlawful-court-nsa> accessed 1 May 2017.
[98] Dominic Rushe, Spencer Ackerman and James Ball, 'Reports that NSA taps into Google and Yahoo Data Hubs Infuriate Tech Giants' <https://www.theguardian.com/technology/2013/oct/30/google-reports-nsa-secretly-intercepts-data-links> 1 November 2017.
[99] Jay Newton Small, 'US Allies Still Angry at Snowden's Revelations of US Spying' (*4 October 2013*) <http://nation.time.com/2013/10/04/u-s-allies-still-angry-at-snowdens-revelations-of-u-s-spying/> accessed 1 November 2017.
[100] DJ Pangburn, 'Surveillance for All: Foreign Governments' Responses to the PRISM Scandal Are Telling' (*20 June 2013*) <https://motherboard.vice.com/en_us/article/surveillance-for-all-foreign-governments-responses-to-the-prism-scandal-are-enlightening> accessed 1 May 2017.
[101] See section 1.1.1, 1.2.2. and 1.3.1.1.
[102] EDPA, 'Statement: EDPS Following the NSA Story' (*10 June 2013*) <https://edps.europa.eu/sites/edp/files/edpsweb_press_releases/13-06-10_statement_nsa_en.pdf> accessed 1 May 2017.

data of the US persons or only at non-US persons, including EU persons and (2) whether access to such data is strictly limited to specific and individual cases, based on a concrete suspicion, or if information is also accessed in bulk.[103]

Then, President Barack Obama claimed that the surveillance PRISM programmes did not apply to US persons and were lawful since they were originally authorised by FISA court and then-US DNI James Clapper, the head of the NSA and other intelligence agencies, also explained that PRISM was justified under Section 702 of the FISA Amendments Act of 2008.[104] The UK agencies also insist that their access to personal data was carried out in accordance with a strict legal and policy framework which ensured that their activities were authorised, necessary and proportionate.[105] This statement was very controversial and was later opposed in many court cases.[106]

Germany, which is considered to be the most aggressive nation in protecting individual privacy cancelled a Cold War-era administrative agreement with the US and the UK for protecting personal privacy.[107] The European Parliament accused the NSA of systemic infringement of privacy rights of EU data subjects and called for a profound overhaul of the transatlantic legal framework of cooperation in the field of counter-terrorism.[108]

1.3.3.2 The Schrems Case

The important court case responding to the Snowden revelations is the case of

---

[103] A29WP, *Letter by A29WP to Vice-President Vivian Reding* (7 June 2013).
[104] Peter Baker, 'Obama Calls Surveillance Programs Legal and Limited' (*7 June 2013*) <http://www.nytimes.com/2013/06/08/us/national-security-agency-surveillance.html> accessed 1 May 2017; Carl Franzen, 'President Obama on NSA Spying: Congress has Known about It and Approved for Years' (*7 Jun 2013*) <https://www.theverge.com/2013/6/7/4406416/president-obama-on-nsa-spying-congress-has-known-about-it-and> accessed 1 July 2017.
[105] BBC, 'Hague: Law-abiding Britons have nothing to fear from GCHQ' (*9 June 2013*) <http://www.bbc.co.uk/news/uk-22832263> accessed 1 May 2017; See Regulation of Investigatory Power Act 2000, Section 8(4).
[106] The example can be seen in the investigatory power Case No. IPT/13/92/CH and Case No. IPT/13/77/H.
[107] BBC, 'Germany Ends Spy Pact with US and UK After Snowden' (*2 August 2013*) <http://www.bbc.co.uk/news/world-europe-23553837> accessed 1 May 2017.
[108] European Parliament, *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* (Committee on Civil Liberties, Justice and Home Affairs, 21 Febrary 2014).

Maximilian Schrems v Data Protection Commissioner.[109] On 25 June 2013, Mr Schrems, an Austrian law student and Facebook user, made a a complaint to the Irish supervisory authority (Data Protection Commissioner (DPC)), to prohibit Facebook Ireland from transferring his personal data from Facebook's Irish subsidiary to servers located in the US. He contended in the compliant that in the light of the Snowden revelations in 2013, concerning the activities of the US NSA, the law and practice of the US did not offer sufficient protection against surveillance conducted by the US public authorities of the data transferred from the EU to the US.

The Irish authority rejected the complaint on the ground that the Commission considered that under the Safe Harbor agreement, the US ensured an adequate level of protection of the personal data transferred. Mr. Schrems appealed this decision before the Irish High Court. The court decided to stay the proceedings and to refer the question of whether the national supervisory authority can conduct his or her own investigation of the adequacy of DP in a third country to the CJEU.

The CJEU held in its its ruling of 6 October 2015 that

(1) a national supervisory authority had the right to investigate the adequacy of data transfers under the Safe Harbor agreement or any other arrangements concluded pursuant to an adequacy decision by the Commission for that matter;[110]

(2) the Safe Harbor Agreement was invalid due to the fact that it failed to comply with the requirement laid down in the Article 25(6) of DPD.[111]

The CJEU observed that the Safe Harbor scheme was applicable solely to the US undertakings which adhere to it, and US public authorities were not themselves subject to it.[112] Furthermore, national security, public interest and law enforcement requirements of the US prevailed over the Safe Harbor scheme, so that US undertakings were bound to disregard, without limitation, the protective rules laid down by that scheme where they conflict with such requirements. Moreover, the criteria for determining which

[109] Case C-362/14 *Maximillian Schrems v Data Protection Commissioner*, CJEU, Judgment of 6 October 2015.
[110] ibid para 66.
[111] ibid para 98.
[112] ibid para 79-98.

situation should be necessary to meet such requirements was not explicitly provided.

Following that, on 1 December 2015, Mr. Schrems filed a renewed complaint with the Irish DPC based on Facebook's use of standard contractual clauses (SCCs) to authorise EU-US data transfers.[113] Mr. Schrems also updated his complaint with the DPC against Facebook in the previous compliant, and contended that US surveillance law was not in line with the requirements laid down by EU law including the judgment of the CJEU in the Safe Harbor decision. Schrems argued that SCCs also incorporated exceptions for illegal mass surveillance, so that SCCs failed to provide an adequate legal protection necessary to allow data transfers.

However, the Irish DPC found that it did not have the ability to declare the clauses invalid under EU law. The Irish DPC brought the case back before the Irish High Court and then the High Court issued its ruling on 3 October 2017 which included referring to the CJEU the question of whether the SCCs are valid under the EU Charter. We now await the CJEU decision.[114]

The absence of a valid legal basis for the lawful transferring of personal data from the EU to the US, where almost all the popular CSPs are based, is a big challenge for the US CSPs to ensure a high level of personal DP regarding the EU DP law. This situation would pose privacy risks to the EU data subjects, and then could potentially make the EU data subjects hesitate to entrust their data with the US CSPs and CSPs who have their servers located within the US.

As cloud computing could be a major driver of economic development, the US has been attempting to rebuild trust between the EU and US, which then could help facilitate data exchanges between both by introducing a range of legal instruments to ensure an adequate level of protection to the privacy rights of the EU data subjects when their data entrusted with the US CSPs, as follows.

1.3.4 US Legal Frameworks After Snowden and Schrems

[113] Complaint against Facebook Ireland Ltd by Schrems, 1 December 2015 < http://www.europe-v-facebook.org/comp_fb_ie.pdf> accessed 1 November 2017.
[114] Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, No, 4809 P, the Irish High Court, Judgment of 3 October 2017.

1.3.4.1 Judicial Redress Act 2015

This Act was enacted on 26 February 2016 to rebuild the credibility of the US with the EU after the leak of the US NSA mass surveillance.[115] This was part of the package of measures that was designed to address the problems about the EU - US data transfers. It extends the privacy protection which the Privacy Act of 1974 provided only to US persons to non-US persons by allowing them to sue a designated US Federal agency in the US courts for unlawful access/disclosure of their personal data transferred from the EU to the US.

A civil action under the Act can be brought against:

(1) a US agency that intentionally violates the conditions for disclosing an individual's records without the individual's consent;

(2) a designated US agency (by the Department of Justice (DOJ)) that refuses an individual's request to amend his or her records or;

(3) a designated US agency that refuses to permit an individual to review records that pertain to him or her.[116] The remedies include both monetary damages and injective relief.[117]

However, before the EU data subjects can bring a civil action against the US agencies, the DOJ will need to designate countries or organisations whose data subjects may pursue such civil remedies. This Act sets out criteria which should be met before the designation, including when the person's country or organisation (1) has appropriate privacy protections for sharing information with the US, as provided in an agreement with the US or as determined by DOJ; (2) permits the transfer of personal data for commercial purposes between its territory and the US; and (3) has DOJ-certified data transfer policies that do not impede the US national security interests.[118]

Nevertheless, the country's designation may be revoked if it: (1) does not comply with a privacy protection agreement, (2) no longer has appropriate privacy protections for sharing information, (3) fails to meet requirements for transfers of personal data for

[115] The Judicial Redress Act 2015. Pub.L 114-126.130 Stat 282, 5 USC 552a, 4 February 2016.
[116] Judicial Redress Act, Section 2(a).
[117] Judicial Redress Act, Section 2(a)(b)(c).
[118] Judicial Redress Act, section 2(d)(1).

commercial purposes, (4) no longer meets the DOJ's transfer policy certification requirements, or (5) impedes the transfer of information to the US (for purposes of reporting or preventing unlawful activity) by a private entity or person.[119]

The entry into force of the Judicial Redress Act of 2015 is seen as a major step towards getting agreement on a new EU-US privacy framework: "Privacy Shield", which replaced the EU-US Safe Harbor Agreement declared invalid by the CJEU in *Schrems*.[120] It also paves the way for the signing of the new DP framework for EU-US law enforcement cooperation: "EU-US DP Umbrella Agreement".[121]

1.3.4.2 USA Freedom Act of 2015

This Act was passed on 2 June 2015 to implement reforms to the US Patriot Act, which had expired the day before.[122] It extended Section 215 of the Act, which allows the NSA to collect a variety of business records that are relevant to national security investigation. But it imposed some new limits on the bulk collection of telecommunication metadata on US persons by US NSA, and further requires the NSA to identify and show a "specific selection term" which identifies a person, account, address, or personal device or any other specific identifier.[123]

This Act also moves government accountability forward by increasing the transparency of its proceedings and rulings, by requiring the DNI, in consultation with the AG, to either declassify, or publish an unclassified summary of, each decision, order, or opinion issued by the FISA Court or the Foreign Intelligence Surveillance Court of Review that includes a significant construction or interpretation of any provision of law.[124] Moreover, this Act provides companies many options to report publicly the aggregate number of FISA orders or National Security Letters (NSL) they receive from

[119] Judicial Redress Act, Section 2(d)(2).
[120] See section 1.4.1. and chapter 3, section 2.3.3.
[121] See section 1.4.2.
[122] The Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015. Pub.L 114-23. 129 Stat 268, 2 June 2015.
[123] Freedom Act, Section 103, 107(4), 201 and 501(4).
[124] Freedom Act, Section 108 and 402.

the Government, as well as the number of users accounts targeted by these orders to their users.[125]

1.3.4.3 USA Liberty Act of 2017

This Act was introduced on 6 October 2017 to reform and reauthorise Section 702 of the FISAA 2008 (which was set to expire in December 2017) which allow warrantless surveillance on communications of both US and non-US users for foreign intelligence purposes.[126] The main component of this Act is to

(1) provide better privacy protection to US persons by requiring the government to obtain a court order based on probable cause in order to access or share the contents of US communications that were incidentally collected under Section 702, regardless of the purpose of the search or the agency conducting it;[127]

(2) strengthen protections for US civil liberties by prohibiting collection of "about" communications of US users and requiring collection only of communications that are "to" or "from" a target;[128]

(3) prevent government abuse of US users by requiring agencies that query Section 702 databases to keep records of queries, and requiring the government to officially retain unmasking requests in order to allow the Congress to exercise oversight and ensure that US persons' privacy is protected; [129]

(4) require the DNI to report to Congress twice each year on the number of US persons whose communications are incidentally collected, the number of unmasking requests that involve US persons, and the number of requests by the intelligence community that resulted in dissemination of unmasked US person identities;[130]

(5) improve oversight of the government surveillance regime and increase government transparency by improving the operations of the Privacy and Civil Liberties Oversight Board (PCLOB), which acts as a watchdog over the federal government' s

[125] Freedom Act, Section 601-605.
[126] The USA Liberty Act, H.R. 3989, 115th Congress (2017).
[127] Liberty Act, Section 101.
[128] Liberty Act, Section 102.
[129] Liberty Act, Section 103.
[130] Liberty Act, Section 106.

national security tools to ensure that they do not endanger civil liberties of *the US persons*.[131]

1.3.4.4. USA Rights Act of 2017

The Act, which was introduced in the Senate on 25 October 2017, also provides a reform to Section 702 of the FISAA 2008.[132] The main concept of this Act is to

(1) prohibit the government from searching, without obtaining a court order, through communications collected under Section 702 to deliberately conduct warrantless searches for the communications of specific US persons, except for emergency situations;[133]

(2) prohibit "reverse targeting", which is the targeting of a non-US persons in order to acquire the communications of the US person who is known to be communicating with that non-US persons;[134]

(3) prohibit the government from collecting communications and phone records that are "about" the target (US person). Collection would be limited to communications that are "to" or "from" the target;[135]

(4) provide new accountability and transparency provisions, such as improving the role in oversight of electronic surveillance by empowering any amicus curiae appointed to advise the FISC to raise any issues with the court at any time;[136]

(5) address challenges litigants face in establishing standing to challenge surveillance under Section 702;[137]

(6) provide transparency around the number of US persons surveilled under Section 702, unless the government says that conducting such an estimate is not feasible, and if it is not, the government should provide a public explanation.[138]

1.3.4.5 FISA Amendments Reauthorisation Act of 2017 (FISAAR)

[131] Liberty Act, Section 202.
[132] The USA Rights Act, H.R.4124, 115th Congress (2017).
[133] Rights Act, Section 2.
[134] Rights Act, Section 3.
[135] Rights Act, Section 6.
[136] Rights Act, Section 8.
[137] Rights Act, Section 11.
[138] Rights Act, Section 18.

The Act was introduced in the Senate on 25 October 2017 to re-authorise and extend government surveillance power under section 702 of the FISAA 2008.[139] The key component of this Act is to

(1) establish in statute that the FISA can re-authorise the government to conduct "about" collection, which the FISA Court can do now without legislation, but this Act requires the AG to notify Congress and imposes a 30-day period during which Congress could pass legislation preventing the collection from restarting. And if Congress fails to pass such legislation within a 30- day period, the "about" collection can restart.[140] It also expands current "about" collection authorities by allowing for immediate unintentional acquisition of "about" communications, and also expands the types of permissible targets to facilitates, places, properties, and premises.[141]

(2) prevent the use of Section 702 to collect data that is "to", "from", or "about" a US person in a criminal proceeding against *that US person*, unless the proceeding concerns e.g. national security, death, kidnapping and serious bodily injury and in this case, there is no limit whatsoever on the use of Section 702 data in any investigation, or civil or administrative proceeding.[142]

1.3.4.6 Clarifying Lawful Overseas Use of Data Act of 2018 (Cloud Act)

This Act was enacted in 2018 to require CSPs to preserve, back up or disclose 'the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber in their possession when asked to do so under warrant, regardless of where the data is stored and who create it.[143]

Since the data held in the cloud may cross international borders, US CSPs can find themselves caught in the middle between the conflicting DP laws for various different countries. This Act allows them to file a motion to quash or modify the US legal process for extraterritorial data where the CSP reasonably believes that (1) the customer or

[139] The FISA Amendments Reauthorisation Act, S.2010, 115th Congress (2017).
[140] FISAR, Section 3.
[141] FISAR, Section 3(1)(3).
[142] FISAR, Section 6.
[143] The Clarifying Lawful Oversea Use of Data Act 2018, HR 4943, 115TH Congress, 2D Session.

subscriber is not a US person and does not reside in the US; and (2) that the required disclosure would create a material risk that the CSP would violate the laws of a qualifying foreign government.[144]

There are two main types of provision set out by this Act. Firstly, the provisions that allow the US government to compel CSPs – like Google or Amazon to hand over a user's content or metadata, even if it is stored in a foreign country.[145] Secondly, the provisions that allow the US AG, with the concurrence of the Secretary of State, to enter into "executive agreements" with foreign governments (which met the requirements set out by this Act, e.g. the foreign government has adopted appropriate procedures to minimise the acquisition, retention, and dissemination of information concerning US persons subject to the agreement).[146] This would allow each foreign government to acquire users' data stored by US CSPs, responding to the foreign government orders, regardless of where the data is stored, without following each other's privacy laws.

This Act came out of the controversy over the Microsoft Ireland disclosure case. It had a direct impact on the case of *Microsoft vs US* as it resolved the question at the heart of this case in favour of the government's ability to reach the data stored extraterritorially. This dispute arose in 2013 when the US government sought to obtain customers' email accounts from Microsoft through an SCA warrant, which was issued by the US District Court for the Southern District of New York, as there was probable cause to believe that the account was being used to further illegal drug trafficking.[147] Due to the fact that such information was stored on company servers located in Dublin, Microsoft moved to quash the warrant with respect to the information stored in Ireland. The magistrate judge denied Microsoft's motion, the District court affirmed it, and then Microsoft appealed for the Second Circuit. On appeal, a panel of the Court held that requiring Microsoft to disclose the electronic communications in question would be an

[144] Cloud Act, Section 3(b).
[145] Cloud Act, Section 3-4.
[146] Cloud Act, Section 5(b)(2).
[147] United States v Microsoft Corporation, the US District Court for the Southern District of New York, Judgment of 25 April 2014.

unauthorized extraterritorial application.[148]

Soon after the Cloud Act was passed, the US government obtained a new warrant for Microsoft under the Cloud Act, seeking the same materials pursuant to the Cloud Act as those which it had previously sought under the SCA and finally, on 17 April 2018, the Supreme Court of the US vacated the Second Circuit decision and remanded the case to the lower court for dismissal.[149]

1.4. EU-US Agreements

1.4.1 EU-US Privacy Shield (Privacy Shield)

In July 2016, this Shield was adopted by the Commission to replace the EU-US Safe Harbor Agreement, which was ruled to be invalid by CJEU in the case of *Maximillian Schrems v Data Protection Commission.*[150] Within a year, more than 3000 companies had subscribed to this Shield, such as Amazon, Google, Facebook and Dropbox.

It aims to protect the fundamental rights of anyone in the EU whose personal data is transferred to the US within a private sector. It also includes written commitments and assurance by the US that any access by public authorities to personal data transferred under the Shield on national security and law enforcement grounds will be subject to clear conditions, limitations and oversight, preventing generalised access.[151] The bulk collection of personal data could only be used under specific preconditions, e.g. to identify and assess new or emerging threats, and needs to be either "mass" or "discriminate" as possible.[152]

It also details the condition for access and use of personal data by the public authorities for law enforcement and public interest purposes, e.g. requiring a court-

[148] United States v Microsoft Corporation, 829 F.3d 197, the US Court of Appeals for the Second Circuit, Judgment of 9 December 2016.
[149] United States v Microsoft Corporation, No 17-2, the US Supreme Court, Judgment of 17 April 2018. The analysis of this Act can be seen in section 2.3.3.
[150] European Parliament, *Commission Implementing Decision of 12.7.2016 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield* (Brussels, 1272016 C(2016) 4176 final); *C-362/14 Maximillian Schrems v Data Protection Commissioner* (CJEU, 6 October 2015). See chapter 3, section 2.3.2.4.
[151] Privacy Shield, Art 67- 90.
[152] Privacy Shield, Art 71 – 73.

ordered warrant upon a showing of "probable cause".[153] Moreover, the US Secretary of State creates the redress possibility for Europeans through an Ombudsperson mechanism, who will handle and solve complaints or enquiries raised by EU individuals in this sector.[154]

1.4.2 EU- US Umbrella Agreement (Umbrella Agreement)

This agreement came into force in February 2017 as a comprehensive DP framework in exchanging personal data between EU Member States LEAs, an authority of EU (e.g. Europol and Eurodac) and US federal LEAs for ensuring a high level of DP and enhancing cooperation in relation to the prevention, investigation, detection or prosecution of criminal offenses, including terrorism.[155] It can also apply to transfers organised between private parties and competent authorities, as long as an agreement is in place between the US and the EU or its Member States.[156] This agreement is not in itself a legal instrument for personal data transfer between EU and US LEAs but it supplements, where necessary, DP safeguards in existing and future data transfer agreements or national provisions authorising such transfers.[157] It explicitly excludes the activities of intelligence agencies for safeguarding national security.[158]

Transfer of personal data shall be for specific purposes authorised by the legal basis set out by this agreement and could not be further processed beyond compatible purposes.[159] An onward transfer must be subject to the prior consent of the competent authority of the country which had originally transferred such personal data.[160] The parties shall provide in their applicable legal frameworks specific retention periods for records containing personal data, the object of which is to ensure that personal information is not retained for longer than is necessary and appropriate.[161] The EU data subjects are entitled to seek access to their personal data and request it to be corrected if

[153] Privacy Shield, Art 125-135.
[154] Privacy Shield, Art 116-124; The Analysis of Privacy Shield can be seen in section 2.3.4.
[155] Privacy Shield, Art 1.
[156] Privacy Shield, Art 3(1)
[157] Privacy Shield ,Art 1(3).
[158] Privacy Shield, Art 3(2).
[159] Privacy Shield, Art 6.
[160] Privacy Shield, Art 7.
[161] Privacy Shield, Art 12.

it is inaccurate.[162] Moreover, they have the right to seek judicial redress before the US courts in case of the US authorities denying their access to or amendment of, or unlawfully disclosing the records containing their personal data.[163]

2. ANALYSIS: WHAT LEGAL PROBLEMS AFFECTING TRUST IN CLOUD COMPUTING EMERGE FROM THESE EU AND US LEGAL FRAMEWORKS?

After the 9/11 attack carried out in the US in 2001, followed by a range of attacks in the EU, e.g. Spain (2004), Paris (2015), there has been an increasing demand to obtain access to personal data held by online service providers for the purpose of law enforcement and national security. Online surveillance has long been understood as a critical process for preventing, detecting, investigating and prosecuting terrorist and other serious crimes.

However, especially since the covert mass surveillance programmes such as PRISM were disclosed in 2013, as canvassed earlier, huge attention has fallen on the activities of LEAs and NIAs mid fears of mass violation of privacy rights. The PRISM scandals have been a "wake-up call" showing arguably how urgent it is to set up international standards for privacy protection in the field of law enforcement and national security so that the balance between protecting national security and preserving the privacy right of individuals is set in a transparent and proportional way.

As discussed in chapter 1, the fundamental problem is that data residing in the cloud can be physically stored at various places across the world and moves and is re-copied dynamically, so that there is a possibility that the LEAs and NIAs will seek to obtain access to the data relating potentially to criminal activity located in various different countries. As explained earlier, this thesis looks at the general impact this possibility has on the trust of users, but only focuses in legal detail on problems arising when US LEAs and NIAs gain access to the data of EU data subjects stored with US CSPs (whether located within or outside the US).[164]

---

[162] Privacy Shield, Art 16-17.
[163] Privacy Shield, Art 19.
[164] See the main focus of this thesis in the Introduction Chapter.

Having canvassed the complex web of laws now dealing with this issue both at international, and at domestic US and EU level, this section will consider how effective these legal frameworks are at safeguarding the privacy of EU cloud users of US controlled cloud services, and thus how well their trust and confidence in such services is enabled.[165]

In particular, this section will evaluate the adequacy of the privacy protection that US legal frameworks provided to EU data subjects before the Snowden revelations broke and the *Schrems* case was heard; and provide an analysis of whether the legal frameworks proposed after these events, do indeed work satisfactorily to improve the current situation, in order to rebuild trust between the EU and the US.

2.1 Defects in US Legal Instruments that Lead to Mass Surveillance

The traditional and formal legal approaches that allow US LEAs to acquire personal data of the EU data subjects (foreign data) for law enforcement purposes – namely the Convention on Cybercrime and MLAT applications - do not seem to be working effectively to protect privacy of the EU data subjects.[166]

The Convention on Cybercrime has been considered to be largely a symbolic policy and to have only a limited effect on combating cyber crime.[167] In the US, this Convention has provoked many controversial issues, especially the lack of adequate privacy protection provided by this Convention and the unjustified expansion of investigative powers, resulting from the absence of the dual criminality required by this Convention.[168] The US thus set forth some reservations and declarations, with its

[165] See the issue of trust in cloud computing in Chapter 2.
[166] See section 1.1.3 and 1.1.4.
[167] Nancy E. Marion, 'The Council of Europe's Cyber Crime Treaty: An exercise in Symbolic Legislation' (2010) 4 IJCC 699, 702.
[168] Elspeth Wales, 'Draft Council of Europe Cybercrime Convention Upsets Civil Rights Bodies' (2000) 2000 Computer Fraud and Security 7, 7; See generally in Ryan M.F. Baron, 'A Critique of the International Cybercrime Treaty' (2002) 10 CommLaw Conspectus 263; Amalie M. Weber, 'The Council of Europe's Convention on Cybercrime' (2003) 18 BTLJ 425, 438; Laura Huey and R.S. Rosenberg, 'Watching the Web: Thoughts on Expanding Police Surveillance Opportunities Under the Cyber-Crime Convention ' (2004) 45 CJCCJ 597; Susan W. Brenner, 'The Council of Europe's Convention on Cybercrime ' in J. M. Balkin and others (eds), *Cybercrime: Digital Cops in a Networked Environment* (New York: New York University Press 2007).
Dual Criminality is a requirement not only with extradition, but also with the transfer of criminal proceedings and with execution of foreign sentences. See more at

instrument of ratification, claiming that this Convention did not require implementing legislation in the US due to the fact that the existing US federal law is adequate to satisfy the Convention's requirements for legislation.[169]

MLATs meanwhile in practice have been subject to many problems.[170] Firstly, its procedure can be costly, slow and cumbersome.[171] Secondly, it can bring about legal uncertainties due to the fact that it consists of a flexible and discretionary system that requires a case by case consideration by the requested Member State and its procedure does not always involve a court authorisation regarding the information collected.[172] Thirdly, it is only designed for sharing information bilaterally and it may not exist for certain countries. Fourthly and crucially, the activities of NIAs for national security purposes are always excluded from the scope of such international legal frameworks, but the surveillance of the online communication of foreigners has been an invaluable source of information for US NIAs.

As a result, it is observable that agencies may feel constrained to turn to other less globally acceptable routes or unacceptable routes to obtain access to the personal data held in private sector. They may choose to make a direct request to US CSPs to obtain access to such data, or - somewhat less legally or even illegally - launch a "back door search" to a cloud server located within or outside the US for law enforcement and

---

<https://www.cambridge.org/core/journals/israel-law-review/article/double-criminality-in-extradition-law/9236841068D61B41E7ACFECDC867B1F6>acesssed 1 January 2018.

[169] George W. Bush, 'Message from the President of the United States Transmitting: Council of the Europe Convention of Cybercrime, Which was Signed by the United States on November 23, 2001 ' (*The White House, 17 November 2003*) <https://www.congress.gov/108/cdoc/tdoc11/CDOC-108tdoc11.pdf> accessed 1 November 2017.

[170] See generally in CoE, *T-CY Assessment Report: The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime* (Strasbourg, France, 3 December 2014).

[171] Cristos Velasco, Julia Hörnle and Anna-Maria Osula, 'Global Views on Internet Jurisdiction and Trans-border Access : Current Developments in ICT and Privacy/Data Protection' in Serge Gutwirth, Ronald Leenes and Paul De Hert (eds), *Data Protection on the Move* (Law, Governance and Technology Series 24, Springer 2016) 469.

[172] See generally in Gail Kent, 'The Mutual Legal Assistance Problem Explained ' (*Center for Internet and Society, Stanford Law School 23, Febraury 2015*) <http://cyberlaw.stanford.edu/blog/2015/02/mutual-legal-assistance-problem-explained> accessed 1 November 2017; Kevin Lonergan, 'Peering Through the Cloud: How Cloud Data Can be a Vital Component of Law Enforcement' (*8 March 2016*) <http://www.information-age.com/peering-through-cloud-how-cloud-data-can-be-vital-component-law-enforcement-123461065/> accessed 1 September 2017.

national security purposes.[173]

The Snowden revelations clearly show that this is what the US NSA and other agencies did either directly or indirectly (e.g. the UK GCHQ): (inter alia) acquired foreign data by making directly requests to CSPs or by backdoor searching to cloud servers controlled by private companies who are based in the US (Google, Yahoo, Microsoft etc.). Although, the US argued that all these activities were lawful and were supervised by federal judges and authorised by Congress (under Section 702 of FISA), all such activities do seem to pose privacy risks to the EU data subject whose personal data stored in the cloud. These activities thus still created anger, controversy and loss of trust, even though possibly authorised by US laws.[174]

2.2 Are EU Users of US Cloud Services Given Sufficient Privacy Protection by US Legal Frameworks? If Not, Why Not?

2.2.1 Absence of EU-Level Privacy Standards in US Legal Frameworks Generally

Both the US and the EU maintain that they are committed to upholding individual privacy rights and ensuring the protection of personal data. However, these issues have long been sticking points in US-EU economic and security relations, in part because of the differences in expectations of legal protection and the legal regimes around privacy protection in the US and the EU.[175]

Firstly, in Europe, privacy is recognised as a human right which applies to all individuals, regardless of their identity, and to both the private and the public sectors.[176] This right has long been developed through many legal instruments, such as the ECHR

[173] In this case, it can be seen from the SCA case discussed in section 1.3.2.3 that whether CSPs can voluntarily give the data to such agencies remains questionable. See also the discussion about transparency reports which now do show millions of data requests made by governments in chapter 5 section 1.2.2.
[174] A29WP, *Working Document on Surveillance of Electronic Communications for Intelligence and National Security Purposes* (14/EN/WP228, Adopted on 5 December 2014, 2014) 7-9.
[175] See generally in Paul M. Schwartz, 'The EU-U.S. Privacy Colission : A Turn to Institutions and Procudures' (2013) 126 HLR 1966; See section 1.1.1. and 1.1.2.
[176] See section 1.1.1.

and the EU Charter.[177] Any interference in the exercise of this right by a public authority is allowed only if specific conditions are fulfilled, especially if it is necessary in a democratic society in the interests of national security or if it is for the protection of the rights and freedoms of others.[178]

On the other hand, in the US, there is no concept of privacy rights as human rights equivalent to the one that is entrenched in the EU laws.[179] There is only the concept of privacy rights as civil rights of US persons, in which the Fourth Amendment of the US Constitution provides protection only to US persons.[180] The Fourth Amendment is the main legal instrument guaranteeing US persons' privacy against intrusion by the government.[181] It prohibits unreasonable searches and seizures by the government, with certain exceptions (e.g. obtaining a valid warrant from the court or if there is a probable cause for a warrantless search).[182]

Secondly, in the EU, there are comprehensive legal frameworks on privacy protection with regard to the processing of personal data in both the private and the public sectors. In the private sector, the legal frameworks on DP (the DPD, succeeded by the GDPR) allow Member States to adopt legislative measures to restrict the scope of DP rights of users if such a restriction meets their conditions, such as when such a restriction constitutes a necessary, appropriate and proportionate measure within a democratic society, e.g. to safeguard national security and public security.[183] In the public sector, the legal frameworks on DP (e.g. the Framework Decision and the PCJDPD) impose specific rules governing the activities of LEAs and set out the legal

[177] See section 1.1.1 and 1.2.2.
[178] See section 1.1.1.
[179] Els de Busser, *Data Protection in EU and US Criminal Cooperation: A Substantive Law Approach to the EU Internal and Transatlantic Cooperation in Criminal Matters between Judicial and Law Enforcement Authorities* (1 edn, Maklu Pub 2010) Chapter 1.
[180] Thomas McIntyre Cooley, *The General Principles of Constitional Law in the United States of America* (Boston: Little, Brow, and Company. 1880); Milton R. Konvitz, 'Privacy and the Law: A Philosophical Prelude' (1966) 31 Law & Contemp Prob 272; Louis Brandeis and Warren Samuel, 'The Right to Privacy' (1890) 4 Harv L Rev 193; Dorothy J. Glancy, 'The Invention of Right to Privacy ' (1979) 21 Arizona L Rev 1.
[181] Steven Erlanger and Jack Ewing, 'Differing Views on Privacy Shape Europe's Response to U.S. Surveillance Program' (*14 June 2013*) <http://www.nytimes.com/2013/06/15/world/europe/differences-on-privacy-shape-europes-response-to-us-surveillance.html> accessed 1 May 2017.
[182] See section 1.3.1.1.
[183] See chapter 3, sections 1.1 and 1.2.

basis allowing the transfer of personal data to the authorities in third countries or to international organisations, e.g. if it is necessary for the prevention, investigation, detection or prosecution of criminal offences.[184]

In contrast, in the US, there is no such single and comprehensive legal framework in both the private and the public sectors. The privacy protection guarantees are in general sector-specific.[185] The US legal framework is both piecemeal, variable and not comprehensive.[186] For example, the Privacy Act of 1974, which is a federal law, provides a protection against privacy intrusion by public agencies, but this protection is only restricted to US persons.[187] It allows agencies to disclose information, which is contained in a system of records by any means of communication to other agencies, including foreign agencies, if there is prior written consent of the data subject or if it is pursuant to one of twelve statutory exceptions, e.g. disclosure to federal LEAs, after receiving a written request made by the head of such an agency. The Federal Trade Commission Act of 1914 (FTC Act) is also a federal law on consumer protection that prevents unfair methods of competition and unfair or deceptive acts or practices affecting both offline and online commerce.[188] It allows the Commission to share confidential information in its files with foreign LEAs in consumer protection matters, subject to appropriate confidentiality assurances.[189]

2.2.2 Absence of an Adequate Level of Protection in US Legal Frameworks for EU Persons Especially

As has been discussed above in section 1.3, there are many US legal frameworks for protecting privacy of the EU data subjects that permit the US LEAs and NIAs to obtain access to personal data of EU data subjects stored in cloud servers located both within

[184] See sections 1.2.1 and 1.2.3
[185] See generally in Amitai Etzioni, *The Limits of Privacy* (New York : Basic Books 1999); David Banisar and Simon Davies, 'Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments' (1999) 18 J Marshall J Computer & Info L 1, 13-14.
[186] European Parliament, *The US Legal System on Data Protection in the Field of Law Enforcement Safeguards, Rights and Remedies for EU Citizens* (May 2015)19.
[187] See section 1.3.2.1.
[188] 15 U.S.C. §§41-58.
[189] 15 U.S.C, Section. 57b-2.

and outside the US for law enforcement or national security purposes. However, the extent to which the privacy rights of the EU data subjects are protected is however variable.

The most worrying issue for EU data subjects are based on the way in which those law differentiate between the US persons and everyone else.[190] The US legal frameworks that cause considerable anxiety regarding the privacy to EU data subjects are the FISA of 1978, the USA Patriot Act of 2001 and the FISAA of 2008, which contain provisions which allow for discrimination between US and non-US persons.[191]

The USA Patriot Act of 2001 was considered to be an overreaction that allowed the Federal Government to jeopardise the democracy by permitting the bulk collection of telephone metadata, or the mass collection of basic call-log information, from telecommunications company(section 215).[192]

Originally, the FISA was a legal framework which governs surveillance for national security purposes. It authorised warrantless electronic surveillance to acquire the content of communications transmitted by means of communications used exclusively between or among non-US persons.[193] But this would affect US persons, when they are engaged in communication with non-US persons.

Many criticisms are aimed at FISAA, Section 702 which grants additional powers to US agencies to obtain transnational access to foreign data that is located outside the US, for a period of up to one year under specified limitations, including (1) not intentionally targeting any person known at the time of acquisition to be *located in the US*; (2) not intentionally targeting person reasonably believed to be located outside the US if the purpose of such acquisition is to target a particular, known person reasonably believed to *be in the US*; (3) not intentionally targeting a *US person* reasonably believed to be located outside the US; (4) not intentionally acquiring any communication as to

[190] Judith Rauhofer and Casper Bowden, 'Protecting Their Own:Fundamental Rights Implications for EU Data Sovereignty in the Cloud' (Edinburgh School of Law Research Paper Series No 2013/28) 13.
[191] Ian Brown and Douwe Korff, 'Foreign Surveillance: Law and Practice in a Global Digital Environment' 3 EHRLR 243, 243.
[192] Wolf C, 'An Analysis of Service Provider Transparency Reports on Government Requests for Data' A Hogan Lovells White Paper, 27 August 2013 <http://www.hldataprotection.com/files/2013/08/Hogan-Lovells-White-Paper-Analysis-of-Transparency-Reports.pdf> accessed 16 May 2016.
[193] 50 U.S. Code § 1881.

which the sender and all intended recipients are known at the time of the acquisition to be *located in the US*.[194]

It can be seen that these limitations aim to protect US persons, rather non-US persons. Moreover, the requirements imposed by such legal frameworks for carrying out electronic surveillance on US persons do seem to be higher than those for non-US persons. For example, while the electronic surveillance conducted on non-US persons can be approved for the period of up to one year, such surveillance conducted on US persons can only be approved for no more than 90 days.[195] Accordingly, this Act has been considered to constitute a legal basis for the blanket surveillance of non-US persons, involving less judicial oversight and which tend to go far beyond the purpose of national security.[196] This would increase the potential for excessive government access to data and insufficient procedural protections.[197]

As a result, entrusting personal data with US-based CSPs, or with CSPs who have their data centres located within the US has caused major concerns among the EU cloud users, as their personal data may neither be protected at the same level as their own government provides, nor be protected at the same level as the US government provides to the US persons.[198]

The main cause of this problem is not US agencies breaking laws per se, but arises from the structurally inadequate level of privacy protection that US laws provide to EU cloud users. And this has made a huge impact on trust of EU cloud users in cloud

---

[194] 50 USC 1881a (FISAA, Section 702 (b)).
[195] See 50 U.S.C. § 1805(d)(1).
[196] 50 U.S. Code § 1881a. European Parliament, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU: Mapping Member States' Legal Frameworks* (Luxembourg: Publications Office of the European Union, 2015).
[197] Winston Maxwell and Christopher Wolf, *A Global Reality: Governmental Access to Data in the Cloud: A Comparative Analysis of Ten International Jurisdictions* (A Hogan Lovells White Paper, 23 May 2012) 1-2.; Christopher Wolf and Bret Cohen, 'Pan-American Governmental Access to Data in the Cloud' A Hogan Lovells White Paper, 17 July 2014 <https://iapp.org/media/presentations/14Academy/A.CSA14_Fact_or_Fiction_HO2.pdf> accessed 12 May 2016, 1-2.
[198] See generally in Steve M. Young, 'Verdugo in Cyberspace: Boundaries of Fourth Amendment Rights for Foreign Nationals in Cybercrime Cases' (2003) 10 Mich Telecomm Tech L Review 167; Fred H. Cate, James X. Dempsey and Ira S. Rubinstein, 'Guest Editorial : Systematic Government Access to Private-Sector Data' (2012) IDPL 1 ; Paolo Balboni and Enrico Pelino, 'Law Enforcement Agencies's Activities in the Cloud Environment: a European Legal Perspective' 22 ICT Law 165.

computing as can be clearly seen from empirical evidences, especially after the Snowden revelations.[199] Consequently, the EU and the US have tried to improve this situation by proposing a number of legal instruments to limit the US government's access to data of EU cloud users stored with US CSPs and to allow EU cloud users to sue US companies in US courts about the misuse of their data. The analysis of the proposed legal instruments can be seen in the following section.

2.3 Assessing the Post-Snowden and Schrems Legal Landscape

This section will evaluate how effective are the legal instruments which have been proposed after the mass surveillance disclosed in 2013 by the US and the EU in dealing with the lack of an adequate level of privacy protection for EU data subjects and with a view to rebuilding trust between the EU and the US.

2.3.1 Judicial Redress Act of 2015 - analysis

The Judicial Redress Act of 2015 was enacted to create new rights for EU data subjects to bring actions against US agencies under the Privacy Act of 1974, to obtain civil remedies for damage resulting from unlawful disclosure of their personal data and to obtain access to and correct government records about themselves.[200] Nevertheless, even for US persons, the Privacy Act is considered to be limited in the rights to redress that it gives and it is riddled with limitations and exceptions.[201] Federal agencies can exempt themselves from almost all of the requirements of the Privacy Act with respect to investigatory material compiled for law enforcement purposes, even when the data subjects have never been accused or suspected of any crime.[202]

Under the interpretation of the Privacy Act adopted by Judge Seeborg's ruling in many cases (e.g. *Edwards Hasbrouck v US Customer and Border Protection*), additional Privacy Act exemptions could be promulgated at any time in the future and applied even

[199] See chapter 2, section 2.2.
[200] See sections 1.3.2.1 and 1.3.4.1.
[201] Dimitry Kochenov, Laurent Pech and Kim Lane Scheppele, 'Why the (US) Judicial Redress Act is Worthless' (*The Identity Project*) <https://free-group.eu/2016/02/25/why-the-us-judicial-redress-act-is-worthless/> accessed 1 April 2018.
[202] Privacy Act 1940, 5 U.S.C. §552a(b).

to requests that have already been made.[203] Nobody can rely on any rights under the Privacy Act that could be retroactively revoked at any time. Therefore, there are few successful examples of litigation against the US government by US persons under this Act.[204] This Act gives US persons inadequate privacy protection. Accordingly, with the Judicial Redress Act, EU data subjects will continue to have even less protection and fewer rights than US persons.

The Judicial Redress Act of 2015 provides only civil remedies and does not include criminal remedies.[205] Some of the provisions are somewhat unclear and they are open to interpretation. Moreover, they contain a number of limitations and exceptions that prevent EU data subjects from exercising their rights as follows.[206]

(1) This Act only applies to natural persons residing in a "covered country" that has been designated by the AG and other cabinet members and this determination is not subject to judicial or administrative review.[207] Therefore, it will not apply in cases where the data transfer takes place before a country became a "covered country" and thus a "covered person" loses his right to sue if the designation of his home country as a "covered country" is revoked by the AG.

(2) An action may only be brought against "a designated federal agency or component", such as the FBI or the NSA under limited circumstances, e.g. if it fails to amend any records regarding particular individuals or refuses to provide individuals with access to their records, and the designation conducted by the AG and other cabinet members is not subject to judicial or administrative review.[208]

(3) The legal bases set out above can be relied upon when an action arises in respect of a "covered record", which includes several types of information, in particular information relating to education, financial transactions, criminal history, etc. However,

---

[203] ibid and Edwards Hasbrouck v US Customer and Border Protection, US District Court for the Northern District of California, San Francisco, C 10-03793 RS, Judgment of 23 January 2013.
[204] Mary Ellen Callahan, Nancy Libin and Lindsay Bowen, *Will the Judicial Redress Act Address Europeans' Privacy Concerns?* (Jenner&Block, March 2, 2016).
[205] Judicial Redress Act, Section 2.
[206] Caroline Gouraud and others, 'U.S. Congress Passes the Judicial Redress Act, but Does It Provide Effective Redress?' (*22 October 2015*) <https://www.reedsmith.com/en/perspectives/2015/10/us-congress-passes-the-judicial-redress-act-but-do> accessed 1 April 2018.
[207] Judicial Redress Act, Section 2(d).
[208] Judicial Redress Act, Section 2(e)(f).

a record will only qualify as a "covered record" where it has been transferred by a public authority of or a private entity within a "covered country" to the US designated federal agency for the purposes of preventing, investigating, detecting or prosecuting criminal offenses.[209] This means that any data relating to EU data subjects which is not actively transferred by public authorities or private entities in the EU to a US designated Federal agency, but is otherwise retrieved or collected by the US agency, is not covered by this Act.

2.3.2 USA Freedom Act of 2015 - Analysis

This Act aims to end the ability of the US agencies to collect telephone metadata in bulk under section 215 of the USA Patriot Act of 2001 and to replace this section with a program that requires the agency to conduct searches in a more targeted manner with a view to strengthening civil liberty safeguards.[210] This Act contains provisions that vary significantly from the USA Patriot Act. Section 501 of this Act eliminates the prospect of Section 215 like bulk metadata collection under NSL authority. It is seen as an improvement on the unamended FISA statute.[211]

However, it is still not a great improvement, since it does not address the concern about what will happen to the data that had already been collected under the USA Patriot Act. [212] This Act fails to exclude any possibilities of government overreach in metadata collection of individuals since it grants authority to continue the acquisition of foreign intelligence information to a period of 72 hours without a court order.[213]

Accordingly, it does not seem to go far enough to curtail the agency's mass surveillance of EU communications revealed by Snowden in 2013.[214] This Act is thus not working to rebuild the trust between the EU and the US because it does not provide

---

[209] Judicial Redress Act, Section 2(h)(3).
[210] See Section 1.3.2.7 and USA Freedom Act, Section 103, 107(4), 201 and 501(4).
[211] See generally in Sergio Suarez, *Is America Safer? The USA FREEDOM Act of 2015 and What the FBI and NSA Have, Can, and Should be Doing* (Law School Student Scholarship, Seton Hall Law, 2017).
[212] Scott A. Boykin, 'The Foreign Intelligence Surveillance Act and the Separation of Powers' (2015) 38 U Ark Little Rock L Rev 33, 46.
[213] USA Freedom Act of 2015, Pub. L. No. 114-23Title VII § (A)(2)(B).
[214] Forsyth B, 'Banning Bulk: Passage of the USA FREEDOM Act and Ending Bulk Collection' (72) Wash L Rev 1307.

any greater privacy protection to EU cloud users.[215] As the American Civil Liberties Union (ACLU) deputy legal director Kameel Jaffer commented on the passage of the Freedom Act of 2015 that…

> The bill leaves many of the government's most intrusive and overbroad surveillance powers untouched, and it makes only very modest adjustments to disclosure and transparency requirements.[216]

2.3.3 Later Legislations of the US - Analysis

The US introduced the US Liberty Act of 2017, the US Rights Act of 2017 and the FISA Amendment Reauthorisation Act of 2017, to reauthorise and reform Section 702 of the FISA, in order to strengthen the protection of individual privacy.[217] But they lag significantly behind in granting equal rights to US and EU persons.[218]

The US Liberty Act of 2017 and the US Rights Act of 2017 aim to prohibit the current suspended practice of "about" collection of the information of US persons and to end the government's practice of conducting warrantless searches through data collected under Section 702 to seek information about US persons. Furthermore, the FISA Amendment Reauthorisation Act of 2017 extends the surveillance power of the US authorities to access communications which simply mention targets, even if they are not the recipients of these messages, and this is considered to be unacceptable, since it is likely to pose some threats to the privacy of both EU and US data subjects.[219]

Apart from that, the Cloud Act of 2018 has recently been enacted to resolve the difficulties that the public agencies had in obtaining remote data through warrants issued

---

[215] Manes J, 'Online Service Providers and Surveillance Law Transparency' (2016) YLJ Forum 343; Emily Berman, 'The Two Faces of the Foreign Intelligence Surveillance Court' (2016) 91 Ind L J 1191, 1191.

[216] See more details, available at <https://www.aclu.org/news/senate-passes-usa-freedom-act>accesed 1 April 2018.

[217] See Sections 1.3.4.3, 1.3.4.4. and 1.3.4.5.

[218] Rainey Reitman, 'USA Liberty Act Won't Fix What's Most Broken with NSA Internet Surveillance' (*October 16, 2017*) <https://www.eff.org/deeplinks/2017/10/usa-liberty-act-wont-fix-whats-most-broken-nsa-internet-surveillance> accessed 1 May 2018.

[219] David Ruiz, 'Whistleblower Protections in USA Liberty Act Not Enough' (*17 October 2017*) <https://www.eff.org/deeplinks/2017/10/whistleblower-protections-usa-liberty-act-not-enough> accessed 1 May 2018.

under the US SCA 1986, in which it does not apply extraterritorially.[220] This Act allows both US and non-US agencies to target or obtain access to the communications data of both US and non-US persons held by US CSPs, regardless of where the data is located. This Act enables agreements between the US and non-US governments, whose agencies are permitted by this Act to directly request data from US service providers without adequate protections for user privacy, so that those agencies can bypass the legal safeguards of the MLATs regime and can circumvent national privacy laws in Europe and elsewhere.[221] This does seem to break the principle of territoriality, the core component of international law, and it will affect information requests that overstep the responding countries' privacy safeguards.[222] This Act seems to signal a potentially dangerous and uncoordinated race to the bottom by allowing US LEAs to ignore EU privacy protection regarding access to data stored in the US. [223] As a result, this Act is seen as a new threat to the privacy of both US and non-US persons.[224]

2.3.4 EU-US Agreement - Analysis

There are two EU-US agreements which have been negotiated for cross-border transfers of personal data from the EU to the US in order to ensure that the level of protection provided to EU data subject rights is essentially equivalent to that under the EU law.[225]

Firstly, the EU-US Privacy Shield aims to apply to EU-US data transfers for commercial purposes; it differs significantly from the Safe Harbor agreement since it also sets out the rules regarding access to personal data by public authorities.[226] It does offer many improvements to the Safe Harbor Framework, especially in the areas of

---

[220] See section 1.3.4.6.
[221] Plimpton D, 'Cloudy with a Chance of Clearing: U.S. Cloud Act and European Response' (*8 May 2018*).
[222] Gottlieb C, 'Cloud Act Establishes Framework To Access Overseas Stored Electronic Communications' (*4 April 2018,*) <https://www.clearygottlieb.com/-/media/files/alert-memos-2018/cloud-act-establishes-framework-to-access-overseas-stored-electronic-communications.pdf> accessed 1 July 2018.
[223] Katitza Rodriguez, 'The U.S. CLOUD Act and the EU: A Privacy Protection Race to the Bottom' (*April 9, 2018*) <https://www.lexology.com/library/detail.aspx?g=987998ec-d8c7-4b0b-b140-6d09e0464553> accessed 1 May 2018.
[224] Drew Mitnick, 'New U.S. Cloud Act is a Threat to Global Privacy' (*7 February 2018*) <https://www.accessnow.org/new-u-s-cloud-act-threat-global-privacy/> accessed 1 May 2018.
[225] See section 1.4.1.
[226] See chapter 3, sections 2.3.2.4 (Safe Harbor) and 2.3.3.2.4 (the EU-US Privacy Shield).

redress, oversight and enforcement, which were weaker in the earlier instrument in order to reflect concerns regarding the mass surveillance disclosed by Snowden in 2013. It describes the extent of permitted interference with fundamental rights and explains the safeguards intended to ensure the effective protection of personal data against possible abuse and unlawful access.

However, how effective this Shield is remains doubtful.[227] On 8 September 2017, the US FTC alleged in three enforcement actions that companies made false claims about their Privacy Shield participation.[228] Furthermore, there are challenges to the Privacy Shield Adequacy Decision in many cases, such as *Digital Rights Ireland v the European Commission* and *La Quadrature du Net and Others v the European Commission*.[229]

The current case was brought by Max Schrems against Facebook, this time challenging the adequacy of protection for personal data transferred from the EU to the US under standard contractual clauses (SCCs) by companies subject to US surveillance law.[230] In this case, experts in US law filed testimony in October and November, 2016. Then, the Irish High Court held a trial lasting several weeks in February and March, 2017. Crucially, the Irish High Court, after a decision taken in October 2017, brought a referral in front of the CJEU on 12 April 2018, with 11 questions over a complaint by Max Schrems questioning whether the Privacy Shield could be used to ensure an adequate level of DP as required by the EU DP law when transferring data to the US and also contain the questions on whether US law allows mass indiscriminate processing in breach of EU law, which aim to determine the legal status of data transfers under SCCs.

---

[227] See generally in W. Gregory Voss, 'The Future of Transatlantic Data Flows: Privacy Shield or Bust?' (2016) 19 J Internet L 8.

[228] The US FTC, 'Three Companies Agree to Settle FTC Charges They Falsely Claimed Participation in EU-US Privacy Shield Framework' <https://www.ftc.gov/news-events/blogs/business-blog/2017/09/ftc-cases-affirm-commitment-privacy-shield> accessed 11 May 2018.

[229] Case T-670/16 *Digital Rights Ireland v European Commission*, the EU General Court (Second Chamber), Judgment of 22 November 2017; Case T-738/16 *La Quadrature du Net and Others v European Commission*, the EU General Court (Second Chamber), Judgment of 9 January 2017, action brought on 25 October 2016.

[230] The Data Protection Commissioner v Facebook Ireland Limited and Maximilian Schrems, No. 4809 P, the Irish High Court, judgment of 3 October 2017.

As can be seen in the first *Schrems* decision, it may be hard to see the CJEU approve this Privacy Shield, which does little to address the court's earlier criticisms of the Safe Harbor Agreement which was ruled to be invalid in 2015. If we would like to see how effective this Privacy Shield is, it is worth considering whether or not it meets the criteria set out by the CJEU in the first *Schrems* decision, which requires it to have in place

(1) the right to request access to and rectification or erasure of personal data collected about the data subjects by public bodies under the terms of EU agreements with third countries;

(2) a means for individuals to seek a remedy and judicial redress where their DP or other fundamental rights are infringed through data transfers conducted on the basis of these agreements;

(3) the powers of the EU Member States to monitor and investigate complaints about breaches of the fundamental rights of EU data subjects; and

(4) restrictions on the generalised retention of the personal data of EU individuals without veritable safeguards, particularly content that can be accessed or used for law enforcement or national security purposes.[231]

Regarding these criteria, attention has been paid to the adoption of the USA Judicial Redress Act of 2015, because it allows EU individuals, to access redress mechanisms in cases of alleged misuse as regards personal data processed under EU-US data transfer agreements. However, as discussed in section 2.3.1, this Act does not provide an effective mechanism to get redress for non-US persons who are subject to a surveillance measure based on Section 702 of FISA since it contains a number of limitations and exceptions that prevent EU data subjects from exercising their rights. Additionally, the USA Freedom Act of 2015, the US Liberty Act of 2017, the US Rights Act of 2017 and the FISA Amendment Reauthorisation Act of 2017 as discussed in the previous section, do fail to prevent the possibilities of the US government overreach in

[231] Case C-362/14 Maximillian Schrems v Data Protection Commissioner, CJEU, Judgment of 6 October 2015, para 95, 96 and 101.

metadata collection of the EU individuals.[232] There are no legally binding commitments ensuring that data collection under FISA Section 702 is not indiscriminate and the access is not conducted on a generalised basis (mass) in contrast with the EU Charter.

Moreover, the Cloud Act of 2018 which extends the abilities of US and foreign LEAs to access the communication data held by private companies, like CSPs and stored in servers outside the US by ignoring the MLATs regime and national privacy laws, does pose some more threat rather than more protection to the data of the EU cloud users.[233]

Accordingly, in July 2018, the European Parliament adopted a resolution which provides a number of persistent concerns on Privacy Shield, e.g. the term "national security" in the Privacy Shield could not ensure that DP breaches can be effectively reviewed in courts to ensure compliance with a strict test of what is necessary and proportionate, and finally determined that the Commission and the US authorities did not set up any action plan to address the deficiencies identified by A29WP in 2017, (there should be guidance about remedies for the data subjects, the self-certification process for companies should be enhanced; and the cooperation between the US authorities within the Privacy Shield mechanism should be adjusted to ensure uninterrupted protection for data subjects' rights and rapid compliance with the Privacy Shield principle) and concludes by calling on the Commission to suspend the Privacy Shield.[234]

Due to the fact that all of the above criteria have not been yet achieved, it can be said that although there are some improvements made by the Privacy Shield, it is likely to end up with the same failing as the EU-US Safe Harbor Agreement because it does not contain any findings in the US of laws and practices limiting interference with the right to privacy and DP (e.g. interference by public authorities for security purposes),

[232] See section 2.3.2 and 2.3.3.
[233] See section 2.3.3.
[234] Adequacy of the protection afforded by the EU-US Privacy Shield, European Parliament resolution of 5 July 2018 on the adequacy of the protection afforded by the EU-US Privacy Shield (2018/2645(RSP)) ; A29WP, *EU – U.S. Privacy Shield – First Annual Joint Review* (17/EN WP 255, Adopted on 28 November 2017).

nor of effective judicial remedies for individuals.[235] As a result, the US CSPS can be compelled to provide access to the US NIAs without proper safeguards, and then trust in the US could not be restored.

There is also the EU-US umbrella agreement, which establishes a minimum level of privacy protection regarding data exchanges for the purposes of the prevention, detection, investigation and prosecution of criminal offences, including terrorism, by providing safeguards and guarantees of lawfulness for data transfers, thereby strengthening fundamental rights and improving EU-US law enforcement cooperation.[236] It does not provide an independent legal basis for such transfers, but instead sets out the basic safeguards that must be in place for such transfers to be lawful by in effect making available the rights created by the Schrems decision. Nevertheless, there are still some problems that prevent this agreement from achieving its objectives as follows.

(1) There are diverging principles of necessity and proportionality between the EU and the US.[237] The preamble States that Parties should recognise principles of proportionality and necessity, as well as relevance and reasonableness 'as implemented by the Parties in their respective legal frameworks'. However, the principles of necessity and proportionality held by the US and the EU may not be the same. This may thus lead to different levels of protection that the US provides to the EU data subjects' rights.

(2) The definition of the "Competent Authority" does seem to be too wide and also to be blurred.[238] Article 2 (5) describes the "Competent Authority" as

> a US national law enforcement agency and an authority of the European Union, and an authority of a Member State, which is responsible for the prevention, investigation, detection or prosecution of criminal offenses, including terrorism.

[235] Monteleone S and Puccio L, The Privacy Shield Update on the State of Play of the EU-US Data Transfer Rule (In-Depth Analysis, PE 625151 – July 2018).
[236] See section 1.4.2.
[237] The European Association for the defence of Human Rights, 'Umbrella Agreement: Not Enough Protection for European Residents' (*31 January 2017*) <http://www.aedh.eu/Umbrella-Agreement-not-enough.html> accessed 1 April 2018.
[238] ibid.

Therefore, all kinds of public authorities, including LEAs and NIAs who transfer data for the purposes set forth in the Agreement, are likely to be subject to this Agreement.

(3) This Agreement applies to personal information transferred between the Competent Authorities of one Party and the Competent Authorities of the *other Party*, or otherwise transferred in accordance with an agreement concluded between the US, the EU or its Member States, for the prevention, detection, investigation and prosecution of criminal offences, including terrorism.[239]

The absence of the definition of the "*other Party*" appears to allow the sharing of data sent by the EU LEAs to the US LEAs with the US NIAs for use in the latter's mass surveillance and data mining operations, as well as the onward transfer of such data to third parties, including NSAs of third countries (for national security issues), which are not subject to this agreement.[240] This could then lead to serious human rights violations of EU cloud users.

(4) The Umbrella Agreement in many respects fails to meet important substantive requirements of EU DP law. Some clarifications are really needed in order to ensure that the level of protection of personal data afforded by the Umbrella Agreement is fully consistent with the EU law. In particular, attention should be paid to the following points:

(a) the definitions of "personal data" and "data processing" differ from the definitions provided by the EU DP law, so that they should be in compliance with the basic requirements of EU DP laws;[241]

(b) there should be a definition of sensitive information;

(c) it allows the omissions notification of information security incidents, violations of data, when such notification may "endanger national security", but this potential danger is not specified.[242] This issue should be clarified in a way that limits as much as possible the omission of notifications, and avoids excessive delays of

[239] EU-US Umbrella Agreement, Art 3(1).
[240] Douwe Korff, 'EU-US Umbrella Data Protection Agreement :Detailed Analysis by Douwe Korff' 14 October 2015 <https://free-group.eu/2015/10/14/eu-us-umbrella-data-protection-agreement-detailed-analysis-by-douwe-korff/> accessed 1 May 2018.
[241] EU-US Umbrella Agreement, Art 1(1)(2).
[242] EU-US Umbrella Agreement, Art 10(2).

notifications in order to support the data subjects in asserting their rights to be informed, as guaranteed by Article 47 of the ECHR (the right to effective remedy and to a fair trial);

(d) the data retention period should be defined more strictly in relation to the purpose pursued;[243]

(e) the restrictions to individuals' access rights are very broad, so that these restrictions should be selectively limited to what is indispensable to preserve the public interests enumerated and to strengthen the obligation of transparency.[244]

All these issues should be improved in a way compatible with the EU constitutional principles, in particular with regard to Article 16 of TFEU and Articles 7 and 8 of the Charter.[245] The WP29 also took the view that there should be further clarification on how the Agreement complies with the EU DP laws and on the oversight measures adopted to ensure that the rights afforded are effective.[246]

Furthermore, it is important that the Umbrella Agreement should be taken in conjunction with the Judicial Redress Act of 2015 and the Privacy Act of 1974, which afford all EU data subjects an effective right of redress in the US courts in the law enforcement context. Nevertheless, as has been discussed above, the Judicial Redress Act and the Privacy Act do not work effectively to provide protection to EU data subjects' rights because the application of both Acts is subject to various limitations and there are a number of preconditions as to the scope of the application, the causes of the action provided and the designation of the agencies covered.[247] And since the national security surveillance programs involving data transfers are specifically excluded from this Umbrella Agreement, the current US surveillance issues have not been properly

[243] EU-US Umbrella Agreement, Art 12.
[244] EU-US Umbrella Agreement, Art 16.
[245] See generally in Will R. Mbioh, 'Do The Umbrella Agreement and Privacy Shield Comply with the "Saugmandsgaard Mandatory Requirements"?' (2017) 20 J Internet L 23.
[246] EDPS, *Opinion 1/2016 Preliminary Opinion on the Agreement Between the United States of America and the European Union on the Protection of Personal Information Relating to the Prevention, Investigation, Detection and Prosecution of Criminal Offences* (12 February 2016).
[247] A29WP, *Statement of the Working Party 29 on the EU – U.S. Umbrella Agreement* (Brussels, October 2016).

addressed by this Agreement yet.[248]

In conclusion, it can be said that there are two main reasons for all the problems discussed above. Firstly, the US does not implement the same standard of privacy protection as the EU. It is evident that the US surveillance approaches do not meet the international standard (the ECHR), and the EU standard (the EU Charter), which is what the EU cloud users expect when they entrust their data with US CSPs. There are no clear rules set out by the US laws that demonstrate an attempt to limit the US agencies when conducting mass surveillance of non-US communications. This may be because the lack of concern of US law for the human rights of non-US users, which then made such surveillance legitimate in the eyes of US NIAs and this was backed by legislation such as FISA. Even after the rash of new legislation after Snowden and *Schrems*, the rights of EU persons about privacy protection, redress and transparency are still questionable. [249]

Secondly, the existing oversight regime for ensuring legal compliance under the US laws does not seem to be effective. This can be a loophole that allows the US agencies to circumvent the lawful approaches set out by the US law, e.g. to obtain a valid warrant, in order to access to the data held in the cloud in an illegal manner. This is one of the critical reasons why the US laws could not work satisfactorily to address the mass surveillance conducted by the US NSA, as was revealed by Snowden.

As a result of all these aspects, many surveys have shown that a number of EU cloud users feel reluctant about adopting a cloud service, especially from CSPs controlled by the US or that have a server located within the US.[250] This is because these issues do have an adverse impact on the three factors for creating trust in cloud computing, as discussed in Chapter 2, section 2.3. Firstly, regarding *transparency and control*, many uncertain issues arise in relation to how their data has been used, by whom and for what purposes, after it has been placed in the cloud, and this situation tends to prevent cloud users from having full control over their data.

[248] Umbrella Agreement, Article 3(2).
[249] See generally in Peter Swire and DeBrae Kennedy-Mayo, 'How Both the EU and the US are "Stricter" Than Each Other for the Privacy of Government Requests for Information ' (2017) 66 Emory Law Journal 671.
[250] See the emperical evidence in chapter 2, section 2.2.

Secondly, regarding *accountability*, these problems create many challenges for CSPs who are involved with the data of EU cloud users in taking responsibility for the stewardship of the data according to the contract they have with the cloud users and to the legal requirements, as the US agencies could launch backdoor access to the data without the acknowledgement of CSPs and data subjects. Thirdly, in relation to *data security*, these issues make it difficult for CSPs to preserve the confidentiality, availability and integrity of the data, due to the fact that CSPs may be forced by US laws to allow US agencies to have access to the data of the EU cloud users, and this situation would then pose some threats to the security of the data of cloud users.

Accordingly, all of these problems now need to be addressed with a view to restoring trust between the EU and the US. However, it might not be easy to find a practical way to address all of these problems, due to many controversial issues potentially being raised relating to political issues and national security issues between countries. Legal solutions, such as encouraging the US to implement a privacy protection standard in accordance with the EU standard and to set out a specific set of data processing rules for law enforcement purposes and for national intelligence services purposes, may be helpful in principle. However, in practice, as Forsyth said that 'there is no perfect place to draw the line between privacy and national security', a line separating the data processing by public agencies for law enforcement (the policing function) and for national security would not be easy to draw.[251] Therefore, a non-legal approach, like to promote cooperation between the EU and the US agencies would be helpful to improve the current situation.[252]

CONCLUSIONS

This chapter has shown that the activities of US LEAs and NIAs in accessing personal data of EU cloud users held within the US controlled cloud, on a covert and mass level, have led to the violation of the rights to privacy of EU cloud users, which in turn leads to

[251] Els De Busser, 'EU Data Protection in Transatlantic Cooperation in Criminal Matters Will the EU be Serving its Citizens an American Meal?' (2010) 6 Utrecht Law Review 86, 98.
[252] Forsyth B, 'Banning Bulk: Passage of the USA FREEDOM Act and Ending Bulk Collection' (72) Wash L Rev 1307, 1341.

an international trust deficit. Cloud computing has been seen as a source for intelligence about criminal and terrorist activities. To investigate, detect and prosecute such crimes, LEAs and NIAs need to obtain access to data residing in the cloud, which can be located in various different countries. Traditionally, the Convention on Cybercrime and the MLAs are the main legal frameworks allowing LEAs to obtain such access. However, this complicated series of bilateral and multilateral treaties has numerous problems that have been well documented. The biggest problem is that the process is simply too slow and cumbersome.

As a result, US LEAs and NIAs have sought access to personal data for law enforcement and national security purposes via more "back door" methods with catastrophic outcomes when revealed to the world. US law has a fundamentally different attitude towards the protection of individual privacy and in particular its constitutional provisions have protected only US persons not foreigners. The Snowden disclosures - and others that have followed - illuminated the fact that US surveillance laws were not compatible with the privacy rights guaranteed by the EU and the ECHR.

Although the US has passed a range of laws to improve the current problems, they do not properly address the concerns of all the interested parties: the privacy concerns of EU data subjects, the requirements of the EU DP law, and the problems of US CSPs who may have to fulfill the requirements of both EU and US laws. The US laws have focused more heavily on strengthening the privacy rights of US persons, rather than the privacy rights of EU persons.

Apart from that, the EU-US Agreement, which are (1) the Umbrella agreement; and (2) the Privacy Shield, do not work satisfactorily to bridge the different level of privacy protection provided by the EU and US laws regarding access to personal data held in the cloud for law enforcement purposes. This result has had and continues to have a negative effect on trust in cloud computing especially of the EU cloud users.

As all of these aspects raise many controversial issues, it may be difficult to address them by using the legal approach of encouraging the US to implement the same level of DP standard as the EU through its legal instruments or achieving a greater coherence of the rules for protecting individuals' privacy against the public agencies

between the EU and US cloud users. The problems remain it is uncertain as to whether the US would agree to do all these. Moreover, if the mass surveillance program is not disclosed, the legal challenges would have been impossible. Accordingly, promoting cooperation between the US and EU agencies, may be helpful to ensure uninterrupted privacy protection for EU data subjects, as well as to combat and prevent crime and terrorisms.

The next chapter proposes a number of potential approaches, both legal and non-legal, for building user trust in cloud computing, which has been damaged by the DP problems discussed in Chapters 3 and 4, with a view to making cloud users, at least to some extent, more confident about placing their data in the cloud. This would also facilitate a free flow of data, advance international relations and foster global economic progress.

CHAPTER 5

SOLUTIONS TO THE LACK OF USER TRUST IN CLOUD COMPUTING

INTRODUCTION

As was discussed in chapters 3 and 4, the use of cloud services poses many risks to the privacy of EU cloud users and these could potentially make cloud users feel reluctant to entrust their personal data to CSPs, especially to those CSPs which are controlled from the US or which have servers located within the US.[1] Therefore, I have argued that problems with the legal protection of users' privacy in the cloud do seem to affect the level of user trust in, and thus uptake of, cloud computing.

Cloud computing has the potential to be a major driver for economic development, especially in developing countries, and it provides cheap services and innovative ranges of services to users and SMEs. Building user trust in cloud computing is thus an urgent task in order to facilitate these commercial and social benefits. However, trust is a very subjective matter. Building trust is not an easy task. In this chapter I will assess (a) legal solutions to this issue and then; (b) non-legal (organisational and technical) solutions which may help if purely legal solutions fail.

This chapter aims to answer research question F: What are the possible approaches for building user trust in cloud computing when it is damaged by the two legal problems relating DP as discussed in chapter 3 and 4 (which bring about privacy and DP risks?) After an introduction, two main types of possible solutions, legal and non-legal, to the lack of trust in cloud computing are proposed. Moreover, limitations when selecting each of the proposed approaches will be discussed. Finally, some conclusions will be drawn.

POSSIBLE APPROACHES FOR BUILDING USER TRUST IN CLOUD COMPUTING

Chapter 2 identified three factors that affect user trust in general, and particularly in the adoption and choice of cloud computing services, namely transparency and control,

[1] See the empirical evidence in chapter 2, section 2.2.

accountability and security.[2] Regarding the empirical evidence provided in Chapter 2, Section 2.2, it can be clearly seen that all of these three factors are important, as they have a direct impact on how willing users are to place their trust in the cloud and then adopt cloud services. [3]

This section will propose possible solutions to fulfil these three factors, in aiming to increase the possibility of users placing their trust in cloud computing and to enhance the adoption of cloud computing.

1. LEGAL SOLUTIONS

This section focuses on the legal solutions to the lack of trust in the cloud that have been drawn only from the GDPR as the main DP law within the EU. This is because this thesis mainly focuses on building trust of EU cloud users (both individuals and SMEs users) who expect that the data held in the cloud will be adequately protected as required by the EU DP law.[4] And as the EU Digital Single Market strategy noted, 'trust in the digital environment is undermined by concerns about whether fundamental rights, in particular the protection of personal data, are being respected, the GPDR also aims to provide a strong and more coherent DP legal framework in order to create trust for developing the digital economy across the internal market'.[5]

Additionally, it can be clearly seen that the three factors for creating trust in cloud computing that were discussed in chapter 2 are also the critical DP principles imposed by the GDPR. Accordingly, it is worth considering the approaches that the GDPR sets

[2] See chapter 2, section 2.3. There is now an entire field called Fairness, Accountability and Transparency (FTA) in relation to algorithmic processing, which is often something delivered via cloud computing. There is also an annual FTA conference dedicated to bringing together a diverse community to investigate and tackle issues relating to the topics of fairness, accountability, transparency, ethics and interpretability in machine learning, recommender systems, the web and other technical disciplines. These three factors for creating and evaluating trust in cloud computing provided in this thesis have been, at least, developed independently but come to much the same kind of conclusion as the FTA project. See <https://fatconference.org/index.html> accessed 1 July 2018.

[3] See more details in chapter 2, section 2.2.

[4] See the main focus of the thesis in the introduction chapter.

[5] GDPR, Recital 7; Commission, 'Commission Staff Working Document: A Digital Single Market Strategy for Europe - Analysis and Evidence Accompanying the Document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Single Market Strategy for Europe, SWD 100 final (Brussels, 6.5.2015 SWD (2015)100 final).

out in order to fulfill those three factors with a view to proposing the possible approaches for building and restoring trust in cloud computing.

The GDPR contains a number of provisions designed to encourage the data subjects to have greater trust in information processing, including cloud services. In particular, it includes provisions that give users rights of transparency and sets out, for the first time, explicit accountability requirements for data controllers (controllers); despite the 1995 version continuing, there have been some alterations demanding duties of security for controllers and data processors (processors).

1.1 Improving Transparency and Control

In fact, transparency is not a new principle. The former EU DP law, which is the DPD also imposed this principle, but it was improved by the GDPR in order to make the use of the personal data more transparent and to increase the ability of data subjects to exercise control over their data. Transparency is intrinsically linked to the principle of fairness and the new principle of accountability introduced by the GDPR.

The GDPR requires that personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subjects.[6] Moreover, it requires all controllers to be obliged to take appropriate measures to provide information and communication relating to the personal data processing of data subjects: (i) in a concise, transparent, intelligible and easily accessible form, using clear and plain language; (ii) in writing "or by other means, including where appropriate, by electronic means"; (iii) in an oral form, when this is requested by data subjects; and (iv) free of charge.[7]

Compared to the DPD, the GDPR requires controllers to provide more information to the data subjects, such as the contact details of the controller, the contact details of the data protection officer, the right to lodge a complaint with a supervisory authority and the period for which the personal data will be stored.[8] However, the absence of the definition of 'in a concise, transparent, intelligible and easily accessible form, using

[6] GDPR, Art 5(1)(a).
[7] GDPR, Art 12.
[8] GDPR, Art 13-14.

clear and plain language' seems to leave room for various interpretations of this concept.[9]

Apart from that, the GDPR supports the ability of cloud users to exercise control over their personal data by providing a range of rights to the data subjects, i.e. the right to access data, to rectification, to erasure of the data and to object to the data processing and it also introduces some new rights, which are the right to data portability and the right not to be subject to a decision based solely on automated processing.[10]

The right to erasure (which is known as the right to be forgotten), which provides the data subjects the right to obtain from the controller the erasure of their personal data without undue delay where the ground applies, e.g. the personal data are no longer necessary in relation to the purposes for which they were collected, has been considered a controversial issue of the GDPR.[11] The right to data portability, which is one of the most ambitious elements of the GDPR, for the first time, provides the data subjects the right to receive their personal data, which the data subjects has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided.[12]

In addition, the GDPR requires that the processing shall be lawful only if the data subject has given consent to the processing of his or her personal data for one or more specific purposes and has the right to withdraw his or her informed consent at any time.[13] It also sets out the conditions for valid consent, which are that it should be any freely given, specific, informed and unambiguous indication of the data subject's wishes

[9] See more details in A29WP, *Guidelines on Transparency under Regulation 2016/679* (17/EN WP260 rev01, Adopted on 29 November 2017, As last Revised and Adopted on 11 April 2018).
[10] GDPR, Art 15-22.
[11] GDPR, Art 17. See Townend J, 'Data Protection and the 'Right to be Forgotten' in Practice: a UK Perspective' (2018) 45 International Journal of Legal Information 28; Bartolini C and Siry L, 'The Right to be Forgotten in the light of the Consent of the Data Subject' (2017) 32 CCR 218. See Case C-131/12 Google Spain SL, Google Inc v AEPD, Mario Costeja Gonzalez, Judgment of the Court(Grand Chamber), 13 May 2014.
[12] GDPR, Art 20. See A29WP, *Guidelines on the Right to Data Portability* (16/EN WP 242 rev01Adopted on 13 December 2016 As last Revised and adopted on 5 April 2017).
[13] GDPR, Art 5(1)(a) and 7.

and it should be in a written form.[14] The problems about consent of the data subjects can be seen in chapter 3, section 2.3.2.1 and 2.3.3.2.1.

1.2 Enhancing Accountability

Apart from the transparency principles which could empowers data subjects to hold controllers and processors accountable, the GDPR introduces an accountability principle that requires all controllers to be responsible for, and to be able to demonstrate, compliance with the DP principles.[15]

Moreover, controllers are, therefore, encouraged to adopt a variety of mechanisms introduced by the GDPR to enhance the transparency and compliance with the GDPR:

(a) the Data Protection Impact Assessment (DPIA) requires controllers, prior to the processing, to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data, especially in the following cases:

(1) a systematic and extensive evaluation of the personal aspects of an individual, including profiling;

(2) processing of sensitive data on a large scale; and

(3) systematic monitoring of public areas on a large scale.[16]

The DPIA must always be conducted when the processing could result in a high risk to the rights and freedoms of natural persons.[17] The A29WP provides ten criteria for which indicating whether the processing bears a high risk to the rights and freedoms of a natural person, including (1) evaluation or scoring ;(2) automated-decision making with legal or similar significant effect; (3) systematic monitoring; (4) sensitive data; (5) data processed on a large scale; (6) datasets that have been matched or combined; (7) data concerning vulnerable data subjects; (8) innovative use or applying technological or organisational solutions; (9) data transfer across borders outside the EU and; (10) when the processing in itself 'prevents data subjects from exercising a right or using a service

[14] GDPR, Art 4(11) and 7.
[15] GDPR, Art 5(2).
[16] GDPR, Art 35-36.
[17] GDPR, Art 35(1).

or a contract' (Art 22 of the GDPR).[18]

(b) Codes of Conduct - the GDPR also encourages controllers and processors to draw up codes of conduct to contribute to proper application of the GDPR, with regard to, for example, fair and transparent processing, public disclosures, security measures and international data transfers and dispute resolution.[19]

(c) DP Certification and DP Seals and Marks - are possible approaches for demonstrating the existence of appropriate safeguards provided by controllers or processors.[20]

Adherence to an approved code of conduct, or an approved certification mechanism, would allow data subjects to quickly assess the level of the DP provided by CSPs and would demonstrate their compliance with the GDPR.[21] These solutions of DP certification, and trust marks and seals are further discussed in the following section (non-legal solutions).

Apart from that, it is mandatory for controllers and processors to designate a Data Protection Officer (DPO), when

(a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

(b) the core activities of the controller or the processor consist of processing operations that require regular and systematic monitoring of data subjects on a large scale; or

(c) the core activities of the controller or the processor consist of processing, on a large scale, special categories of data and personal data relating to criminal convictions and offences.[22]

---

[18] A29WP, Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679 (17/EN WP 248, Adopted on 4 April 2017) 8-9.
[19] GDPR, Art 40-41.
[20] GDPR, Art 42-43.
[21] GDPR, Rec 81.
[22] GDPR, Art 37-38. See also A29WP, *Guidelines on Data Protection Officers ('DPOs')* (16/EN WP 243 rev01, Adopted on 13 December 2016, As last Revised and Adopted on 5 April 2017).

The DPO will play an important role in, for example, monitoring the compliance with the GDPR, providing advice when requested regarding the DPIA and cooperating with the supervisory authority.[23]

1.3 Increasing Data Security

The GDPR is not only continuing with the familiar security principle of the DPD, but is also attempting to provide users with greater control over their own data, which, in turn, encourages them to feel that it is more secure. In the case of new rights, i.e. data portability and erasure, users can actively move their data away from sites they deem as being untrustworthy, or they can actively destroy it.[24]

The GDPR sets out a security principle by requiring both controllers and processors (while the DPD required only controllers) to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, such as pseudonymisation and encryption of personal data.[25] It also requires controllers, without undue delay and not later than 72 hours after becoming aware of it, to competently notify the supervisory authority of the personal data breach and processors are also required to notify the controllers, without undue delay, after becoming aware of a personal data breach.[26]

Regarding all above approaches, it remains unclear as to whether all these approaches will work satisfactorily to achieve the three criteria for creating trust in cloud computing. This is because, as has been discussed earlier in chapter 3 in connection with some provisions of the GPDR, there are a number of problems about the applicability of the GDPR, which would be critical factors that would prevent the GDPR from working effectively to build and/or restore user trust in cloud computing. As a result of this, the non-legal solutions would be helpful as additional mechanisms to ensure the increase of the possibility of users placing their trust in cloud computing. They would help reassure

[23] GDPR, Art 39.
[24] GDPR, Art 17.
[25] GDPR, Art 32.
[26] GDPR, Art 33-34; A29WP, *Guidelines on Personal Data Breach Notification under Regulation 2016/679* (18/EN WP250rev01, Adopted on 3 October 2017, As last Revised and Adopted on 6 February 2018).

cloud users that their data will be adequately protected to at least the same level as is demanded by the EU DP law.

2. NON-LEGAL SOLUTIONS (ORGANISATIONAL AND TECHNICAL SOLUTIONS)

2.1 Improving Transparency and Control

This section will suggest potential approaches that provide cloud users with information related to their data held in the cloud in a clear and understandable way and that also enable users to decide, track and audit how and where their data are being used, by whom and for what purposes as follows:

2.1.1 Cloud Icons/Labels

Icons and the Cloud

Icons could be used in the cloud to help inform the data subjects about privacy-related issues, making the content of the privacy policy, which is a legal document, easier to access and comprehend. Icons could be used to indicate the rights and limitations for data subjects, prominently showing an illustrated abstract and easy access level of the privacy policy and to depict the personal configuration of privacy settings or audience selection of individual pieces of content, for example to directly choose individuals that may, or must not, gain access to the data.[27] Machine-readable privacy policies could be interpreted and translated into icons, supplementing the written privacy policies, pointing to relevant sections, for example by adding them as an initial to a paragraph.

Ideally, the icons should be clear, simple and well designed, in order to be able to convey information by means of one single graphical representation, expressing the relevant content in an understandable manner for wide audiences, even ideally across a different culture.[28] Additionally, the icons should offer at least some valuable information on a first-glance basis for users and point to core issues related to the data processing, in order to enhance users' awareness of how their data is handled or

[27] Holtz L-E, Zwingelberg H and Hansen M, 'Privacy Policy Icons' in Camenisch J, Fischer-Hübner S and Rannenberg K (eds), *Privacy and Identity Management for Life* (Springer 2011) 282.
[28] ibid 279.

processed, and for what purpose.[29] However, this is not an easy task and immediately foreshadows some of the problems that icons have faced in practical deployment.

As discussed previously, cloud contracts (also known as Terms of Service (ToS), Service Level Agreements (SLA), Acceptable Use Policies (AUP) or Privacy Policies), are typically written in a way that is long and convoluted, as well as difficult to understand.[30] Empirical research has shown that data subjects are not able to reliably understand the privacy policies of online service providers in any of the existing formats.[31] One idea to improve the transparency in this area is, therefore, to design and use icons and labels. These have long been used to help in communicating complex factual information to users in an easy-to-grasp approach, and, in the context of cloud computing, they could improve users' awareness and comprehension of the complex factual or legal matters with regard to what is happening to their data.[32]

History and Examples

Adoption of icons for privacy policies and terms in an online environment has a long history. The idea was first proposed in 2006 by Mary Rundle in a Creative Commons-like style, which developed a list of icons depicting the copyright license options.[33] These icons allow data subjects to express their particular privacy preferences regarding how their data should be treated through choices symbolized by a different suite of icons that are elaborated on in a prescription, in order to equip individuals with control over

[29] See generally in Leif-Erik Holtz, Katharina Nocun and Marit Hansen, *Towards Displaying Privacy Information with Icons* (352 IFIP Advances in Information and Communication Technology 338, 2011).
[30] See chapter 1, section 7.2. provides a brief discussion about cloud contractual problems.
[31] Aleecia M MacDonald, Robert W Reeder, Patrick Gage Kelley, L F Cranor, "A Comparative Study of Online Privacy Policies and Formats" (2009) in Privacy Enhancing Technologies, 5672 Lecture Notes in Computer Science.
[32] Roy J. Lewicki and Barbara Benedict Bunker, "Developing and Maintaining Trust in Work Relationships," Trust in Organizations: Frontiers of Theory and Research, Thousand Oaks, CA: SAGE Publications, Inc., 1996, 119-122.
[33] Rundle M, *International Personal Data Protections and Digital Identity Management Tools* (Position Paper Submitted for the W3C Workshop on Languages for Privacy Policy Negotiation and Semantics-Driven Enforcement, Italy, 13 September 2006). The Creative Common License is a copyright license that allows creators to distribute their copyright works depending on their needs. A set of standardised icons, including ones for "attribute" (requiring credit to the author),"non-commercial" (to be used only for non-commercial purposes), "no derivative works" (no changes to be made to the work) and "share-alike" (new creations must be in turn licensed under the same terms), are used to depict the copyright license options. See 'Creative Commons ' <https://creativecommons.org> accessed 1 January 2018.

their personal data.

In 2007, Matthias Mehldau also independently developed a set of 30 icons for data privacy, inspired by the Creative Commons licenses, declaring what type of data is used, how the data is handled, and for what purposes and for how long.[34]

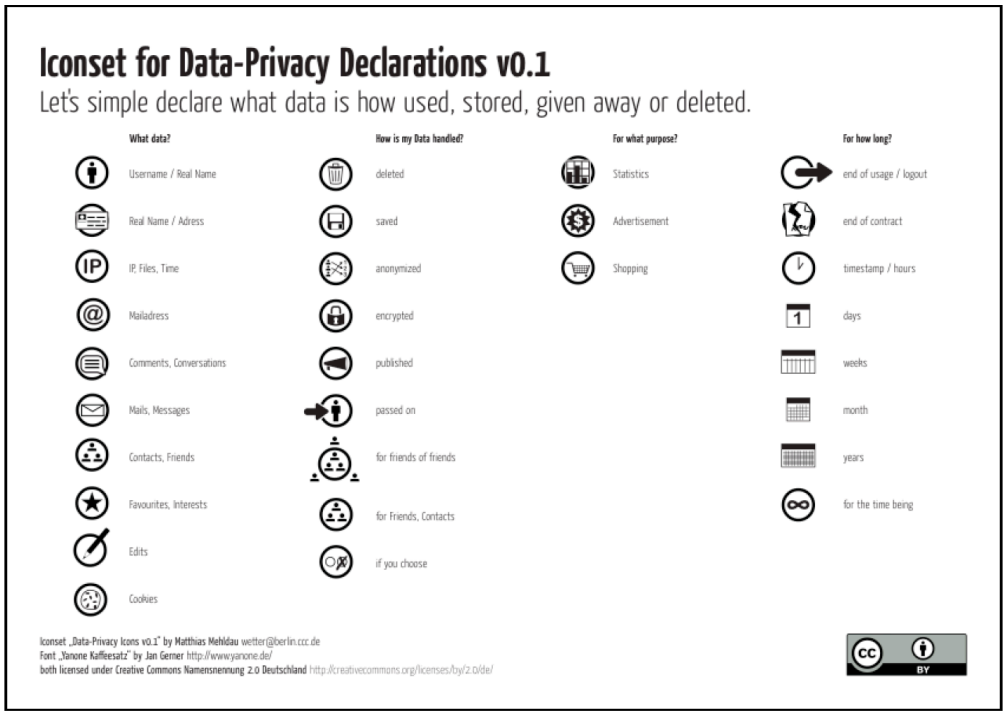

Figure 4. Icons for Data Privacy Declarations by Matthias Mehldau[35]

Primelife, a major EU research project funded by the European Commission's 7th Framework Programme from 2008-2011, included two sets of icons describing, in a neutral way, the privacy policy in considerable detail.[36] Firstly, it is for general usage in e-commerce to depict: (1) data types; (2) specific types of processing and purposes; and (3) how long the user's IP address is stored.[37] Secondly, it is for social networks that

[34] Mehldau M, Iconset for Data-Privacy Declarations V0.1 (2007).
[35] ibid.
[36] 'Privacy and Identity Management in Europe for Life' (2008). <http://primelife.ercim.eu/results/documents/> accessed 1 January 2018.
[37] Fischer-Hübner S and Zwingelberg H, *UI Prototypes: Policy Administration and Presentation – Version 2* (Primelife, 29 June 2010) 34.

depict privacy-related statements referring to the group who will gain access to information, including selected individuals, friends, friends of friends and the general public.[38]

Regarding the Mozzilla privacy icons project in 2010, Aza Raskin attempted to standardise a privacy policy format that would be machine readable and displayed through various different icons, in order to create a simple standard to explain privacy policies.[39]

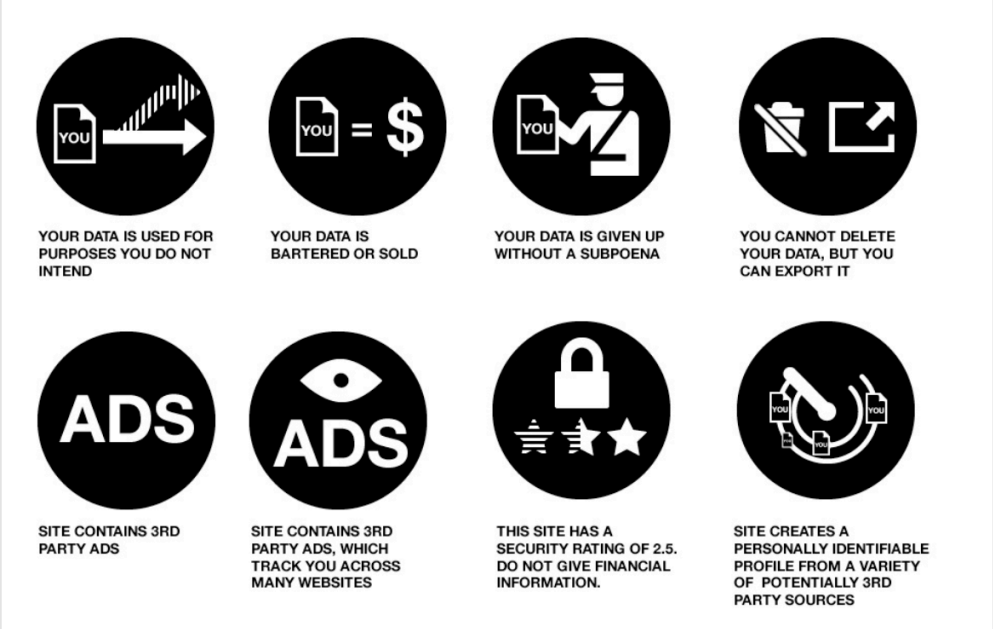

Figure 5. Data Privacy Icons by Aza Raskin[40]

The Privicons were then developed by researchers at Stanford University in the PrimeLife project to convey information about how the data in e-mails should be handled by the recipient.[41] Six icons were developed, appearing as embedded graphics or plain text and which contain a variety of instructions, including "don't print", "delete

[38] ibid 39.
[39] Raskin A, 'Privacy Icons: Alpha Release' <http://www.azarask.in/blog/post/privacy-icons/> accessed 1 January 2018.
[40] ibid.
[41] 'Privicons' <http://www.privicons.org> accessed 1 January 2018.

after reading", "keep internal", "please share", "keep secret" and "don't attribute".[42] These icons could be incorporated into emails, as in the case of browser extensions for Google Chrome that are incorporated into the Gmail user interface.[43]

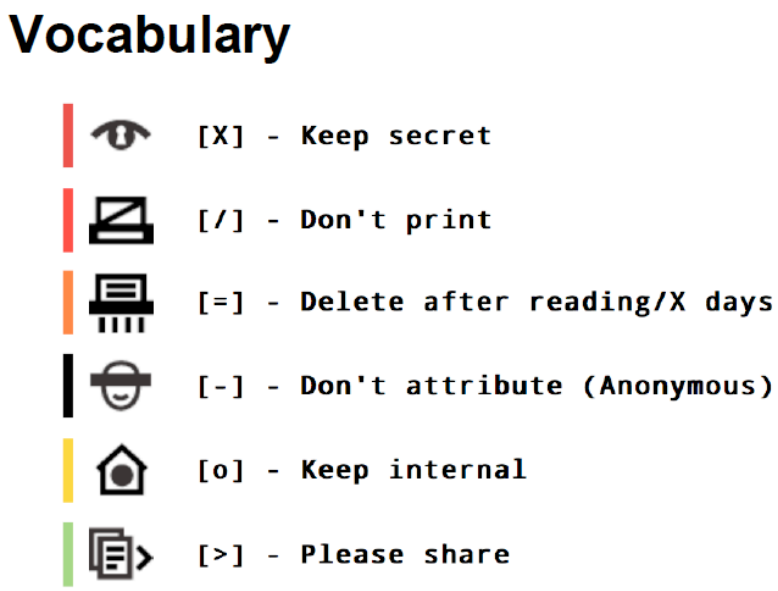

Figure 6. Privicons[44]

In 2014, TRUSTe (currently TrustArc), a well-known privacy/trust seal, and Disconnect, the privacy-advocacy and open source software company, launched Privacy Icons Software (PIS) that includes a set of 9 icons, with green, yellow and red icons signifying the level of concern about the website's privacy policy in each area, which are displayed as a browser add-on, such as desktop browser extensions for Chrome and Firefox for

[42] Forrest E and Schallaböck J, 'Privicons: An Approach to Communicating Privacy Preferences Between Users' Stanford/Berlin November, 2010 <https://www.iab.org/wp-content/IAB-uploads/2011/03/jan_schallabock.pdf> accessed 1 January 2010.
[43] Forrest E, 'Privicons Released: A User-to-User Email Privacy Tool' (*21 November 2011*) <http://cyberlaw.stanford.edu/blog/2011/11/privicons-released-user-user-email-privacy-tool> accessed 1 January 2018.
[44] ibid.

every site they visit and for every search result.[45] These icons indicate: (1) the expected use of data; (2) the expected collection; (3) whether the precise location of users is tracked; (4) the data retention period; (5) children's privacy; (6) do not track compliance; (7) SSL support; (8) heartbleed vulnerability; and (9) TRUSTe certified.[46]

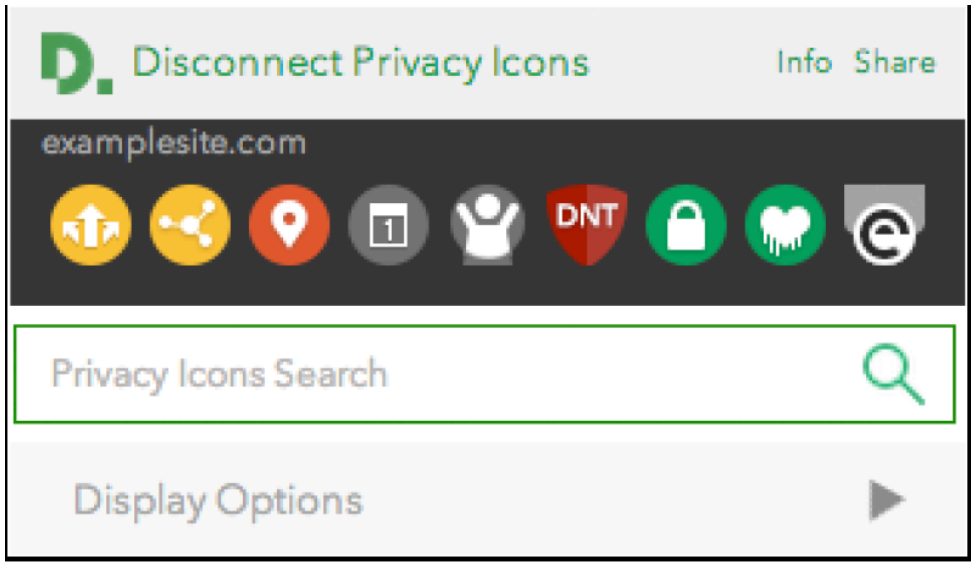

Figure 7. Privacy Icons Software Set[47]

Labels and the Cloud

Compared with icons, labels indicate more specific information about products or services. In an online service, a label could be used to simplify the privacy policies that are often confusing, due to the use of specific terms that users may not understand, or descriptions of activities that people have difficulty in relating to their own use of services. This concept has become popular in the form of labels on food packaging, or energy rating, and has gained widespread recognition around the world, as it could produce a broader understanding of the practices used in designing and defining

[45] 'TRUSTe & Disconnect Introduce Visual Icons to Help Consumers Understand Privacy Policies' (*23 June 2014*) <http://www.trustarc.com/blog/2014/06/23/truste-disconnect-introduce-visual-icons-to-help-consumers-understand-privacy-policies/> accessed 1 January 2018.
[46] See <https://www.trustarc.com/press/category/press-release/ accessed> 1 January 2018.
[47] See <https://disconnect.me/icons>accessed 1 May 2018.

labelling requirements.[48]

History and Examples

The CyLab of Carnegie Mellon University proposed, in 2006, a privacy simplified label that presents privacy related statements as rows in a table to better facilitate comparisons between the policies of various service providers and to reduce the confusion about what data is being collected.[49] This label represents users in relation to four main issues: (1) what kind of information is being collected; (2) who will share or use this information; (3) how this information is used; and (4) contact information to allow users to obtain further information and support.

[48] See generally in Abrams and M Crompton, "Multi–Layered Privacy Notices: A Better Way," (2005) 2 (1) Privacy Law Bulletin 1; G Kelley et al., "Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach" (2010) Carnegie Mellon University, CyLab, Technical Reports, CMU–CyLab.
[49] CyLab Centre at Carnegie Mellon University, 'Privacy Nutrition Labels' (*6 March 2013*) <http://www.openlawlab.com/2013/06/03/privacy-nutrition-labels/> accessed 1 January 2018.

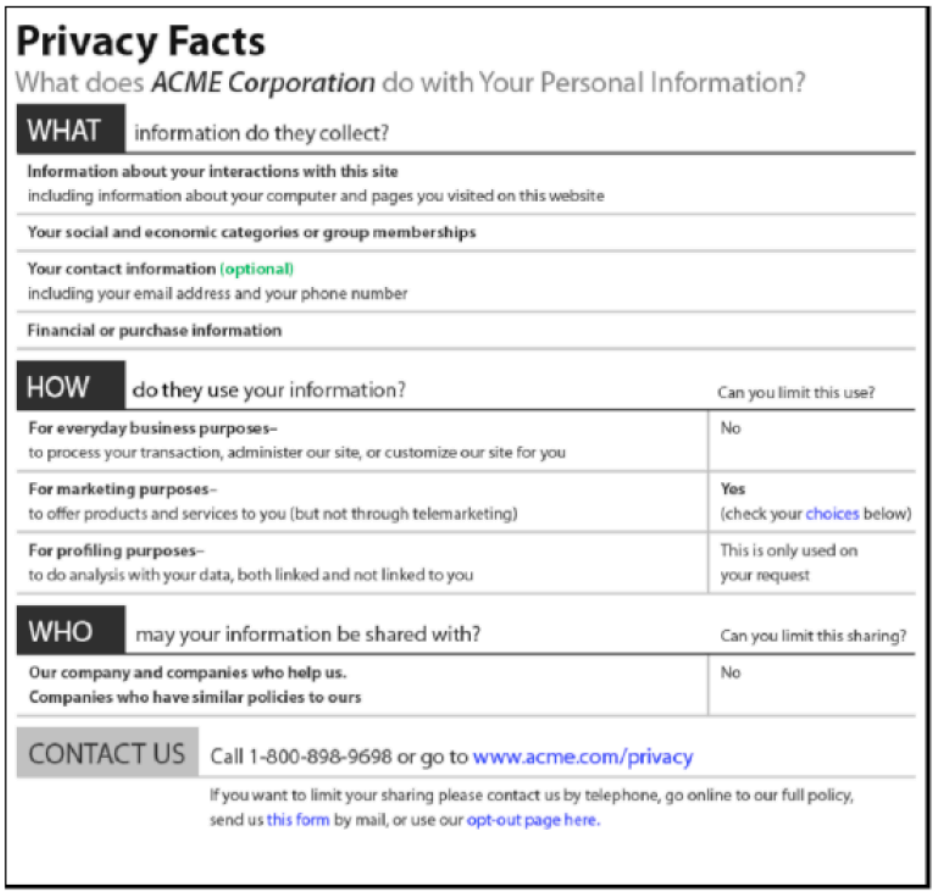

Figure 8. Simplified Privacy Nutrition Label[50]

Later, the Cylab also introduced a simplified grid label to address the issue of there being too much detail provided by a simplified label and, at the same time, to include more detailed information that the privacy policies provide without overwhelming users, by reducing the clutter, introducing colour and simplifying symbols.[51]

[50] Kelley PG and others, *A "Nutrition Label" for Privacy* (Symposium on Usable Privacy and Security(SOUPS), CA, USA, July 2009).
[51] CyLab Centre at Carnegie Mellon University, 'Privacy Nutrition Labels' (*6 March 2013*) <http://www.openlawlab.com/2013/06/03/privacy-nutrition-labels/> accessed 1 January 2018.

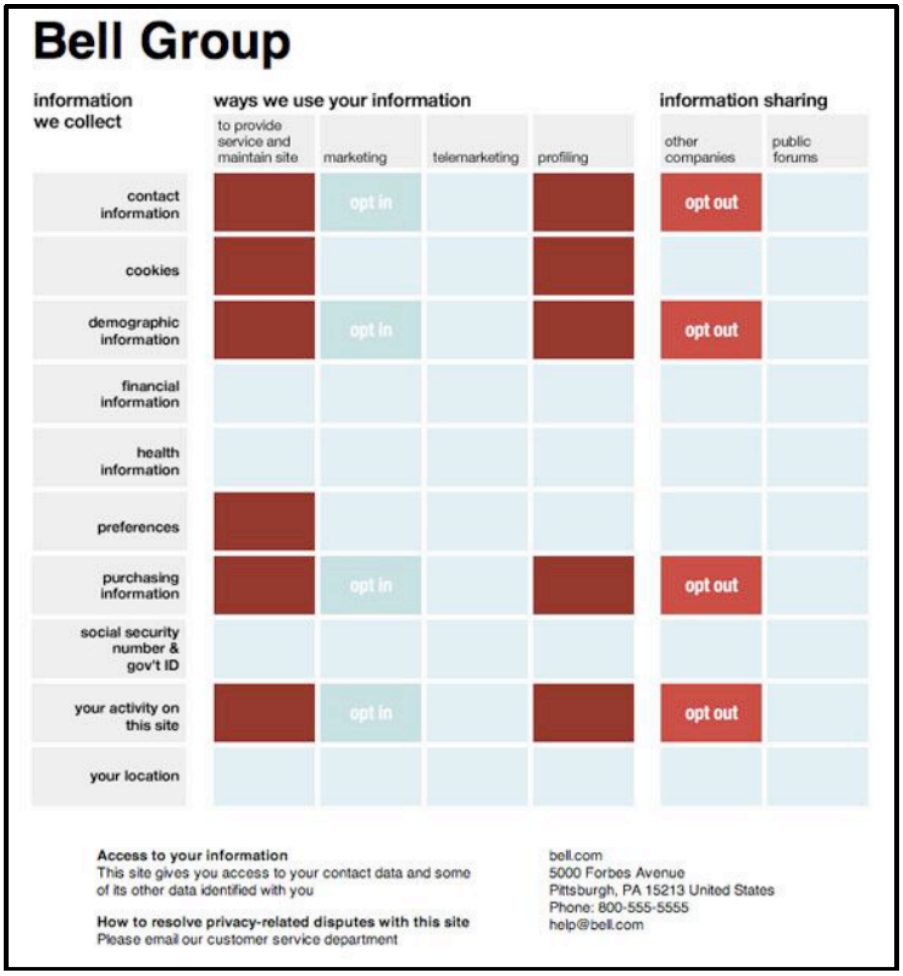

Figure 9. Simplified Privacy Grid Label[52]

In the cloud, labels could be effectively used to create greater transparency in relation to cloud contracts by communicating complex and lengthy privacy policies to users, which is similar to the concept of a nutrition label on food or an energy label.[53] The content of labels should be in common language, short and easily understood by a broad audience, in order to communicate the contents and purpose of the label specifically and to assist

[52] ibid.
[53] As the original point of a system of cloud labels in the legal context has been developed by this thesis, further work about the cloud labels is really needed.

users' recognition.[54] The complete and accurate information provided by the labels would enable users to understand and comprehend the privacy policies more easily and to make accurate privacy assessments.[55]

Van de Werff et al. opined that a dynamic nutrition trust label is useful for helping users to make informed decisions and then to encourage users to place their trust in cloud computing.[56] Lynn et al. also viewed that labels are likely to communicate the trustworthiness of cloud computing to users, as they provide direct information about the services and CSPs, which are the most influential factors for enhancing online trust.[57]

Critique

It remains unclear whether icons and labels work effectively to build trust in cloud computing. Many issues have been raised:

(i) Multiplicity of Icons and Labels

As can be seen above that there is no one definitive set of icons and/or labels and many organisations may have the incentive to create such a set. Accordingly, multiple sets of icons may be used by service providers and may compete for public attention. Because of this multiplicity, no set may achieve a critical mass of recognition, and become both known and trusted by users.

In addition, regarding the PrimeLife project, icons were evaluated in user tests that involved individuals from different cultures (e.g. Swedish and Chinese users). These tests confirmed that there could be cultural differences in the understanding of specific icons.[58] Globally available icon sets may, thus, not necessarily work well in all countries.

---

[54] Corey A. Ciocchetti, 'The Future of Privacy Policies: A Privacy Nutrition Label Filled with Fair Information Practice ' (2009) 26 J Marshall J Info Tech & Privacy L 1.
[55] Labelinsight, *Driving Long- Term Trust and Loyalty Through Transparency* (The 2016 Label Insight Transparency ROI Study).
[56] Werff LVD and others, *Building Trust in the Cloud Environment: Towards a Consumer Cloud Trust Label* (ICDS 2014: The Eighth International Conference on Digital Society).
[57] Lynn T and others, 'Development of a Cloud Trust Label: A Delphi Approach' (2016) 56 JCIS 185.
[58] Graf C and others, Towards Usable Privacy Enhancing Technologies: Lessons Learned from the PrimeLife Project (17 June 2011) 19.

Therefore, there is a great need for standardisation and international harmonisation of icons and labels and a consistent representative language that can facilitate machine-to-machine interoperability to improve the trust in the cloud. Consistency and portability of icons and labels is a critical factor for supporting stable and reliable privacy representations.

(ii) Complexity of Information

Icons and labels in such contexts as privacy and the cloud need to convey specified, detailed information, which may be too complex to understand at a single glance.[59] They have tended to work best in clear simple domains, such as laundry labels or food nutrition.[60] Van den Berg and Van der Hof opined that the use of icons for 'capturing complex, detailed material, such as data protection legislation, in one single image is incredibly difficult'.[61] They also mentioned the Prime Life icon set as involving 'rather complicated drawings' with 'several rather small elements'.

Raskin pointed out that some privacy icons could potentially have poor normative value.[62] The picture that a user gains from icons may be different to the one given by the entire written legal policy. Accordingly, there should be a single page handout providing the meaning of icons and describing the useful terms for helping users to achieve a better understanding. Standardisation and harmonisation could also help in improving this situation.

(iii) Under or Over-Conveying Information – Cognitive Clutter

Nutrition labelling may either sacrifice too much or too little information at once for users. In 2016, the Label Insight Transparency ROI Study, which surveyed more than 2,000 users about their preferences for transparency and how this affects their trust and loyalty towards brands, showed that users want more than just the required product

[59] Holtz, Nocun and Hansen (n29) And Hansen M, 'Putting Privacy Pictograms Into Practice: A European Perspective' (2009) 154GI GI Jahrestagung 1703, 1704-1706.
[60] Lilian Edwards and Wiebke Abel, *The Use of Privacy Icons and Standard Contract Terms for Generating Consumer Trust and Confidence in Digital Service* (CREATe Working Paper 2014/15 (October 2014)).
[61] Van Den Ber B and Van Der Hof S, 'What Happens to my Data? A Novel Approach to Informing Users of Data Processing Practices' (2012) 7 First Monday 1, section 3.
[62] Raskin A, 'Privacy Icons: Alpha Release' (n39).

information on a product's label and they will purchase from, and be loyal to, brands that provide more detailed insights.[63] Moreover, the surveys by Van den Berg and Van der Hof showed that the informational wishes of end users are neatly aligned with the requirements laid down in the DP law. On the other hand, some labels may be more confusing, creating information overload for users.[64] Therefore, finding a balance in the amount of information provided on the labels is needed, in order to provide the best basis for consumers' decision making.

Conclusion

There is a clear problem in that it is difficult to represent the complex information related to privacy and personal data in icons, icons are not used consistently across suppliers, there is a multiplicity of icons, thus any given set is not always recognised by users, and service providers using icons designed by self-regulatory schemes, which dominate the market, can use them without any external audit that guarantees they actually make true and useful representations to users.

In the section below this paper considers methods of certification, trust seals and codes of conduct, all of which may assist in providing an audit of service providers. Certification and trust seal schemes may also involve sanctions for members or signatories, which helps to achieve greater accountability. Should icons and labels be tied to a trust seal or trust mark scheme, as discussed in 2.2.1, then it would be much more plausible for them to be implemented in a useful and fair way.

Arguably, an independent auditor, or ombudsman, could help here, but it is not clear who could play that role (or be funded to do so). The data protection authority (DPA) of each EU Member State could have the role of independently monitoring the use of icons and labels by CSPs, especially as the GDPR does recommend, as noted above, the use of icons to improve transparency. [65] However, this does not necessarily solve the problem of audit and enforcement of the icons or labels used by non EU CSPs,

[63] Insight L, *Driving Long-Term Trust and Loyalty Through Transparency* (The 2016 Label Insight Transparency ROI Study) 2.
[64] Werff LVD and others (n56)161.
[65] ibid.

with whom the loss of user trust is most closely associated.

2.1.2. Transparency Reports

Transparency reports are documents that disclose a variety of statistics about such matters as requests, e.g. for content removal or blocking and governmental requests for access to user data. They were originally introduced by Google as a policy measure to assist them in showing how many copyright take downs were requested by publishers as part of their increasing vulnerability during the "copyright wars".[66] Some now suggest that they can have a key part in building and restoring trust of online users in relation to both the cloud and privacy.[67]

Since the Snowden revelations and other developments that have decreased the user trust in online platforms, such as the ongoing fracas surrounding Facebook and Cambridge Analytica, there has been an increasing tendency to use transparency as a means by which platforms can reassure users and regulators, as well as third parties, such as rights holders.[68] For example, when Google was forced to implement the "right to be forgotten" under the DPD, under pressure from commentators, they have been increasingly giving greater access to data regarding how they are implementing it.[69] Therefore, transparency reports are increasingly ubiquitous.

Transparency reports may be useful in disclosing requests to reveal user data on government application. Transparency reports can, in theory, allow users to find out if

[66] Baldwin P, The Copyright Wars: Three Centuries of Trans-Atlantic Battle (Princeton University Press 2016); 'Requests to Remove Content Due to Copyright' (*Google Transparency Report*) <https://transparencyreport.google.com/copyright/overview> accessed 1 May 2018.

[67] PWC, 'Building Trust Through Assurance Transparency Report 2017' <https://www.pwc.com/gx/en/about/assets/irl-audit-quality-transparency-report-2017.pdf> accessed 1 May 2018; Grieco A, 'Transparency and the Cloud Act: The Importance of Evolving Transparency Reports' (*9 July 2018*) <https://blogs.cisco.com/security/transparency-and-the-cloud-act-the-importance-of-evolving-transparency-reports> accessed 9 July 2018.

[68] It was found that the Cambridge Analytica used personal information harvested from more than 50 million Facebook users without their permission to build system that could target US voters with personalised political advertisements based on their psychological profile. See Meredith S, 'Facebook-Cambridge Analytica: A Timeline of the Data Hijacking Scandal' <https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html> accessed 1 May 2018.

[69] Smith M, 'Updating Our "Right to Be Forgotten" Transparency Report' (*26 February 2018*) <https://www.blog.google/around-the-globe/google-europe/updating-our-right-be-forgotten-transparency-report/> accessed 1 May 2018.

a government (theirs or another) is accessing their data held in the cloud and can alert them about government abuse. This increase in transparency may decrease users' concerns on how their data will be disclosed to any third parties (although it might also arguably increase them). Another advantage might be that it provides a means to hold CSPs to account when they allow covert state access to user data. Finally, transparency reports might allow users to "shop around" to find a service provider they feel they can trust in relation to government access requests.[70]

History

Google was the first major online platform to introduce a transparency report in 2010 and it has been regularly updated since then.[71] This report includes a security and privacy report that presents a number of user data requests from government authorities, alongside the total number of users/accounts specified in those requests in six-monthly increments.[72] Google also sets out common practices for responding to such requests, such as reviewing the request to ensure it satisfies both the legal requirements and Google's policies. Google has connected the law with its practice to ensure legal compliance and to promote its accountability with a view to making users feel that their data will be adequately protected.

Following that, other companies began to add transparency reports, which normally provide (1) the number and types of data requests made by governments (content or non-content); (2) the laws used to justify such requests; and (3) how to respond to such requests. For example, Dropbox has been providing a transparency report since 2012.[73] Microsoft also launched a transparency report in 2013, and it was then redesigned as a "Microsoft Transparency Hub" in 2015, which includes the Law

[70] See generally in Watts S, 'Corporate Social Responsibility Reporting Platforms: Enabling Transparency for Accountability' (March 2015) 16 Information Technology and Management 19.
[71] Google, 'Google Transparency Report' <https://transparencyreport.google.com> accessed 1 January 2018.
[72] Google, 'Requests for User Information' <https://transparencyreport.google.com/user-data/overview> accessed 1 January 2018.
[73] Dropbox, 'Transparency Overview' < https://www.dropbox.com/transparency> and 'Transparency Report'<https://www.dropbox.com/transparency/reports>accessed 1 January 2018.

Enforcement Request Report and the US National Security Order Report.[74] Yahoo, which is currently part of 'Oath' (a digital and mobile media company with more than 50 brands, such as Flickr and Tumblr), publicly publishes a transparency report twice a year.[75]

Critique

Nevertheless, there are some problems that may prevent transparency reports from working effectively to build trust in the cloud:

(i) Voluntary

Despite there being strong public relations incentives to adopt transparency reports, this mechanism remains voluntary, in the sense that it is not required by the law, and the quality and granularity of these reports differ. This can be seen in the two-page transparency report released by Amazon, which provides only the types and volume of data requests and whether or not Amazon allows public agencies to obtain access to the data.[76] There is no information about what data is requested, who makes requests and which products or services are implicated by such requests. Accordingly, the Amazon transparency report is considered to be somewhat deficient and useless.[77]

(ii) Partial and Inconsistent

The requests presented in these transparency reports are only the official and disclosed ones. States may require service providers to not disclose that they have been asked to

[74] Microsoft Transparency Hub <https://www.microsoft.com/en-us/about/corporate-responsibility/reports-hub> accessed 1 January 2018; Microsoft, 'Law Enforcement Requests Report' <https://www.microsoft.com/en-us/about/corporate-responsibility/lerr> accessed 1 January 2018; Microsoft, 'US National Security Orders Report' <https://www.microsoft.com/en-us/about/corporate-responsibility/fisa/ > accessed 1 January 2018

[75] Yahoo, 'Yahoo is Now Part of Oat'. <https://policies.yahoo.com/ie/en/yahoo/privacy/euoathnoticefaq/> accessed 11 January 2018; Oath, 'Transparency Report' < https://transparency.oath.com/index.html> 11 January 2018.

[76] Amazon, 'Transparency Report' <http://d0.awsstatic.com/certifications/Information_Request_Report.pdf> accessed 1 January 2018.

[77] Whittaker Z, 'Amazon Doesn't Want You to Know How Many Data Demands It Gets' (*19 March 2015*) <http://www.zdnet.com/article/amazon-dot-com-the-tech-master-of-secrecy/> accessed 11 February 2018. And 'Amazon's Useless "Transparency Reports" Won't Disclose Whether They're Handing Data From Always-on Alexa Mics to Governments' (*18 January 2018*) <https://boingboing.net/2018/01/18/nunya-bizness.html> accessed 1 February 2018.

reveal certain types of data, such as in an investigation relating to national security. Such "tipping off" laws are common and often heavily sanctioned, e.g. the US SCA 1986.[78] Furthermore, LEAs and NIAs may obtain data by informal or non-overt methods that do not show up in the transparency reports, for example by a "back door" search of the cloud server, without the acknowledgement of CSPs.[79] Therefore, transparency reports, in practice, can never provide full information about the volume, or nature of, access to the personal data held in the cloud by government agencies.

(iii) *Public vs Private Requests in Transparency Reports*

The existing transparency reports now generally provide information about the data requests for law enforcement or security made by public agencies. They also fairly routinely record information about requests relating to data made by private bodies, such as copyright take downs or requests to reveal the identity of users. However, post Snowden, as noted earlier, concerns about data access have moved beyond merely states to the private sector, for example the Cambridge Analytica scandal. It is difficult to perceive how this kind of information relating to the sharing of personal data with the private sector, such as advertisers or application developers, can be mandated. It is a matter of commercial confidentiality often guarded by contracts concerning non-disclosure agreements.

Solutions

It has been suggested that there should be standard for a transparency report.[80] Such standards might require online service providers to notify impacted users of all data requests, which include at least the following information:

(i) who makes a request: courts, LEAs, NIAs or governments;

(ii) how such a request is made: through

(a) *subpoenas* – binding legal demands for information or testimony issued

[78] See more details about the SCA case in chapter 4, section 1.3.2.3.
[79] See chapter 4, section 2.2.
[80] Watts S, 'Corporate Social Responsibility Reporting Platforms: Enabling Transparency for Accountability' (March 2015) 16 Information Technology and Management 19.

by courts, LEAs or grand juries, which are usually without any substantive review by a judge or magistrate;

(b) *search warrants* – may be issued by local, state, or federal courts upon the showing of probable cause and must specifically identify the place to be searched and the items to be seized;

(c) *other court orders* - binding orders issued by local, state, or federal courts, other than search warrants or court-issued subpoenas;

(d) *national security requests* - national security letters and court orders issued under the FISA; and

(e) *non-U.S. requests* - legal demands from non-U.S. governments, and legal orders issued pursuant to MLATs

(iii) what data is requested:

(a) *non-content data* - basic user information, e.g. name, address and email address;

(b) *content data* - contents of communications associated with an account which users create and store on or through online services;

(iv) what is the request about: asking for access to data, to delete data, or to remove data;

(v) when and how often the third parties make a request;

(vi) information about how users can defend themselves against overreaching government demands for their data.

However, the problem remains who will enforce it, what organisation will regulate it and what sanctions could they exert? The concept of Global Network Alliance, which is an ethical body set up by Google and some Non Government Organisations (NGOs) might be helpful in this case.

Moreover, guidelines or common practices on how CSPs deal with data access requests, which are subject to due process, should be followed. These guidelines and common practices may include information about e.g.

(i) obtaining access to different kinds of data – this is subject to different legal

requirements, e.g. private information requires a subpoena or court order and the contents of communications requires a search warrant with a showing of probable cause and a judge's signature. CSPs will receive only the data requests of government agencies which fulfil legal requirements;

(ii) the process of receiving, evaluating and responding to the data requests - all requests should be carefully scrutinised and narrowly interpreted. Only as much data should be disclosed as is necessary to comply with the request; and

(iii) enforcement - the requests may be challenged in the court in order to protect the fundamental rights of users.

In conclusion, transparency reports, while a good step towards transparency to enhance trust of cloud users, are in no way a completes solution to build and restore trust in the cloud. Most obviously, transparency reports merely disclose; they do not give users remedies. Cloud users could not do much with the report. It does not empower cloud users to have full control over their data. This requires *accountability* solutions which we turn to next.

2.2 Enhancing Accountability

This section will suggest two approaches that could be used to guarantee that CSPs will take responsibility for the stewardship of personal data held in the cloud according to contractual and legal requirements and to be liable and to provide remedies for any damages resulting from their non-compliance.

2.2.1. Certification, Trust Marks and Trust Seals

Certification and the Cloud

Certification is defined as:

> a procedure by which a third party gives a written assurance that a product or service is in conformity with certain standards.[81]

[81] Rae AK, Hausen H-L and Robert P, Software Evaluation for Certification: Principles, Practice, and Legal Liability (McGraw-Hill 1995) 2.

Certification is widely used to satisfy users' expectations by confirming providers' commitments to safeguarding data with an obligation to protect it beyond mere legal requirements and making them accountable for any misuse of data.[82]

Briefly, the third party certification process typically consists of the following five main stages;

(i) *Setting Standards* - to enable the evaluation and comparison of products and services under the same rules worldwide;

(ii) *Evaluation* - the process of evaluating products, services and practices through audits (systematic quality verification procedures), including internal audits based on internal standards, internal audits based on third-party standards, and external audits;

(iii) *Issue / Denial of Certification*;

(iv) *Monitoring* - there are two types of monitoring, namely passive monitoring (receiving a complaint when the certified company will be examined under the certifier's programme) and active monitoring (the certifier and the certified company agree to periodic checks);

(v) *Confirmation* (suspension/revocation).[83]

A particular type of certification involves signing up to a trust mark or seal.

Third party certification has a long history of enhancing trust in e-commerce beyond privacy and the cloud. It first emerged in the US in the late 1990s and in the EU a few years later, as a mechanism to solve the problem of trust in e-commerce, which was perceived by consumers in the early days as risky and threatening because it inevitably involved contracting at a distance, often across borders. This led to a lack of direct interaction, loss of credibility in pre-contractual information, and fears of a possibly inadequate level of compliance with laws, as well as worries about effective

[82] See generally in Damon A and others, *Developing Internet Consumer Trust: Exploring Trustmarks As Third-Party Signals.* (AMA Winter Educators' Conference Proceedings, 2003); Aiken KD and Boush DM, 'Trustmarks, Objective-Source Ratings, and Implied Investments in Advertising: Investigating Online Trust and the Context-Specific Nature of Internet Signals' (2006) 34 JAMS 308.
[83] ibid 40-45.

enforcement and the reach of the regulatory authority.[84] So-called Trustmark Organisations (TMOs) became a self-regulatory solution to this problem. [85] They are typically independent third parties that provide a trust mark or seal to assure users that the service providers awarded such certification comply with the TMO's standards, thereby reassuring them of their services.

The oversight regime of certification, trust marks and trust seals, such as TRUSTArc (formally TRUSTe) in the US tend to be self-regulating, since they have little formal regulatory oversight of consumer privacy.[86] However, the FTC has made a role for itself in this area in recent years (as shown below). A regulatory structure for DP already exists in the EU with each State having at least one national DPA; hence, the State or the EU as a whole may sponsor a trust mark, which gives it more "teeth" based on the presence of a state regulator in the background with the power to enforce a breach.[87]

The third party certification of online service providers may cover a variety of topics, such as compliance with regulations, privacy and security measures taken to protect users' data, the clarity of information provided on the website, dispute resolution in cases where a conflict emerges between providers and users, mystery payments and delivery methods.[88] Providers may display the trust mark on their website after their services have been subject to evaluation according to the defined certification criteria. This theoretically makes them more attractive to users. Surveys conducted by the European Consumer Centres' Network have shown that users consider trust marks to be an important aspect of e-commerce and the majority of them tend to trust a service provider that has a trust mark on its website.[89] Trust marks are especially useful for SMEs, which are often little-known brands on their own and require extra measures to

[84] Balboni P, Trustmarks in E-Commerce: The Value of Web Seals and the Liability of Their Providers (T.M.C Asser Press 2009) 30.
[85] ibid 2.
[86] ibid chapter 4.
[87] ibid chapter 3.
[88] See generally in ENISA, On the Security, Privacy and Usability of Online Seals: An Overview (December 2013).
[89] Network TECC, 'Trustmark Report 2013 "Can I Trust the Trustmark?"' October 2013 <http://www.konsumenteuropa.se/globalassets/rapporter/trust_mark_report_2013.pdf> accessed 11 February 2018.

attract users.[90]

Controllers and processors are also encouraged to adopt DP certification, DP marks and seals approved by the European Commission as critical mechanisms to enhance their transparency and demonstrate their compliance with the GDPR.[91]

Trust Marks and the Cloud

According to Lynn et al., trust marks could help to build user trust in the cloud,[92] because they represent an effort to dispel concerns about risk. The existence of a trust mark demonstrates to users that CSPs take their privacy seriously and that they are willing to invest in DP and security in order to mitigate risk, monitor and identify risk and policy violations, manage incidents and provide redress.

TrustArc (formally TRUSTe), which is one of the most popular TMOs in the US, offers a trust mark worldwide to provide real-time verification along with an easy-to-understand user notice that CSPs meet its privacy standards, which are based on globally-recognised privacy requirements, e.g. the Fair Information Practice Principle and Organisation for Economic Co-operation of Development (OECD) Privacy Guidelines.[93] It also provides comprehensive assessments, tracker scanning, finding reports, e.g. risk summaries and free online third-party dispute resolution for complaints reported by users.[94]

EuroPriSe, an independent European TMO, provides privacy certification, which indicates compliance with the EU DP law and meet all EuroPriSe's DP requirements.[95] It also provides reliable best practice recommendations and guidelines about filing a complaint and initiating a dispute resolution procedure. Both TRUSTArc and

[90] Balboni P, Third-Party Liability of Trustmark Organisations in Europe (Tilburgh University Publication, Project 7 November 2008).
[91] GDPR, Rec 81, 100 and Art 42.
[92] Lynn T and others, *The Case for Cloud Service Trustmarks and Assurance-As-A-Service* (International Conference on Cloud Computing and Service Science CLOSER 2013).
[93] See <https://www.trustarc.com/products/enterprise-privacy-certification/> accessed 11 February 2018.
[94] Meissner S, *Privacy Seals: The European Privacy Seal EuroPriSe* (DataEthics: Building Digital Trust – Hellerup, 19 May 2016).
[95] See < https://www.european-privacy-seal.eu/EPS-en/website-privacy-certification-overview> accessed 11 February 2018.

EuroPriSes provide an updated version of the criteria for products and services that already incorporates the new legal requirements of the GDPR, which are publicly available on their websites.

Critique

Nevertheless, third party certification may not be sufficiently effective to build trust in the cloud, since it may be less than perfect for protecting the privacy of users for many reasons.[96]

(i) Lack of Oversight of Self-Regulatory Trust Mark Schemes

The fact that third party certification is easy to obtain and self-regulated, with some non-binding instruments such as standards, means that trust marks may not be as trustworthy as they seem to be.[97] This is widely known as "Regulatory Capture",[98] which is a situation in which sanctions cannot be imposed on CSPs that obtain trust marks for failing to enforce alleged TMO standards (this may be because they pay for trust marks and/or may exchange data with TMOs). An example of Regulatory Capture is TRUSTe (currently TrustArc), which is funded by Microsoft and IBM among others and claims that it is the only organisation that provides comprehensive oversight and a consumer resolution mechanism to assure users that their privacy is protected.[99]

Nevertheless, it fails to take any action for breaches committed by its members and neglects to withdraw its privacy seal from them.[100] For example, in 2017, the New York

[96] See generally in Rifon NJ, Larose R and Choi SM, 'Your Privacy Is Sealed: Effects of Web Privacy: Seals on Trust and Personal Disclosures' (2005) 39 JCA 339; Connolly C, 'Trustmark Schemes Struggle to Protect Privacy' (*26 September 2008*) <http://www.galexia.com/public/research/assets/trustmarks_struggle_20080926/> accessed 12 January 2018.

[97] Balboni P, 'Model for an Adequate Liability System for Trustmark Organisations' (2006) 1 Privacy, and Security Issues in Information Technology 97, 97.

[98] See generally in Charlesworth A, 'Data Privacy in Cyberspace: Not National vs. International but Commercial vs. Individual' in Edwards L and Waelde C (eds), *Law and the Internet* (2rd edn, Hart Publishing 2000); Thaw D, 'Enlightened Regulatory Capture' (2014) 89 Wash L Rev 329.

[99] Charlesworth A, 'Data Privacy in Cyberspace: Not National vs. International but Commercial vs. Individual' (n98) 104; TrustArc, <https://www.trustarc.com/trustarc-partner-program/channel-partner/> accessed 1 May 2018.

[100] See generally in Edekman E, 'Adverse Selection in Online "Trust" Certifications and Search Results' (2011) 10 Electronic Commerce Research and Applications 17.

Attorney General, Eric T Schneiderman, charged TRUSTe (currently TrustArc) with the failure to meet its obligations to adequately assess its members' websites and sanction several privacy breaches by its members, leaving such popular sites as Roblox.com and Hasbro.com vulnerable to the illegal tracking of underage visitors, a practice prohibited under the federal Children's Online Privacy Protection Act (COPPA).[101] Due to the fact that the Federal Trade Commission enforces the FTC Act to take action against companies that engage in unfair or deceptive practices, including the failure to abide by self-regulatory programs they join, the FTC have a state-like role in enforcing breach of privacy policies.[102]

It can be said that most TMOs only provide a passive monitoring system based on complaints from users. Therefore, the chances of failing to detect CSPs that fail to comply with the TMO's code of practice are quite high, which may finally lead to the violation of data subjects' DP rights and lead to a considerable loss of credibility of TMOs.[103]

(ii) Multiplicity of Trust Marks

There is a varied market for multiple trustmarks.[104] Since almost every trust mark has distinctive features, they vary in terms of the standard and degree of scrutiny of self-assessment, renewal of application and procedure to withdraw the mark[105] Most national trust marks are relatively unknown by consumers from other countries, but some are cross-border so that consumers outside the host state may not recognise them.[106] These regional differences cause confusion among users which is contrary to the intention of

[101] In the Master of Investigation by Eric T. Schneuderman, Attorney General of the State of New York, of True Ultimate Standards Everywhere, Inc., d/b/a TRUSTe (Attorney General of the State of New York Beau of Internet and Technology, Assurance No 17-049, 24 March 2017).
[102] See FTC, 'Protecting Consumer Privacy in an Era of Digital Age', December 2010, <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf> accessed 1 March 2018.
[103] Balboni P, Third-Party Liability of Trustmark Organisations in Europe (Tilburgh University Publication, Project 7 November 2008 (n90) 3.
[104] This is the same problem as we have with the multiplicity of icons and labels. See section 2.1.1.
[105] Danidou Y and Schafer B, 'Legal Environments for Digital Trust: Trustmarks, Trusted Computing and the Issue of Legal Liability' (2012) 7 JICLT 212, 214.
[106] Nordquist F, Andersson F and Dzepina EN, *Trusting the Trustmark?* (17th BILETA Annual Conference April 5th - 6th, 2002, Free University, Amsterdam) 2-4.

trustmarks.[107] Accordingly, a minimum criteria to harmonise all national trust marks is really needed.[108] Moreover, the uniform practice/code of conduct of TMOs to allow users to have the possibility to understand and take advantages that trust marks provide is now required.

Apart from that, since cloud users basically rely on the reputation of TMOs, CSPs should adopt trust marks to protect their users' privacy with reliable and trustworthy TMOs that (1) enable CSPs to give their users appropriate control and transparency over the data processing; (2) reassure users that their data will be processed in accordance with codes of conduct; (3) monitor and confirm CSPs' consistent compliance with users' expectations, business policies, regulations and third-party standards; (4) signal CSPs' dependability and trustworthiness to users.[109]

2.2.2 Internal Codes of Conduct or Ethics

The solutions in the section above involved a CSP attempting to instil trust in its users by asking a third party - a certification authority or trust mark – to say that it is trustworthy. Another solution, which is gaining in popularity, is for a company to engage in an internal audit, or publish a list or code of the ethical principles to which it plans to adhere. This internal code of conduct approved by the Commission is the critical mechanism established by the GDPR to help controllers and processors to demonstrate compliance and best practice. Although this is easier and cheaper than using a third party body, it is arguably even more open to lacking true enforcement and being a matter of "something must be seen to be done" rather than a real solution.

For example, Microsoft has established its code of conduct called "standard of business conduct", which includes an ethics and compliance programme that contains a description of the principles that guide its behaviour for building trust with its

[107] Commission, EU Online Trustmarks Building Digital Confidence in Europe: Final Report (2012) 6.
[108] ibid.
[109] Lynn T and others, *The Case for Cloud Service Trustmarks and Assurance-As-A-Service* (International Conference on Cloud Computing and Service Science CLOSER 2013) (n92) 5.

customers[110] The President and Chief Legal Officer serves as the Company's Chief Compliance Office and the violation of this standard may lead to disciplinary action, up to the termination of employment. Meanwhile, Hewlett Packard(HP), an information technology company, imposes quite strong ethical rules with the aim of developing robust privacy regulations that are globally-interoperable by being committed to complying with all applicable laws and regulations to protect the privacy of users wherever it operates, especially the GDPR.[111] It has also established a compliance programme, which is supported by open door reporting and complaint investigation procedures.

Google distributed its codes of conduct to employees under its unique motto "Don't be Evil" which aims to provide users unbiased access to information, focus on their needs and give them the best services. However, Google does abandon it in many situations, e.g. reintroducing a censorship search engine to China (dragonfly); selling face recognition to the army/pentagon – which then caused an employee backlash and Google withdrew from doing it.[112] Google may believe that this motto could encourage more employees to question and protest the company's future projects that may be in an ethically grey area, so that this motto was removed sometime in early May 2018.[113] The latest version of Google code of conduct does not mention the GDPR, but rather provides its commitment to protect data as required by the applicable law.[114] The compliance will be monitored by a steering committee and an audit committee. Nevertheless, how effective will this be remains unclear.

---

[110] Microsoft, 'Ethics & Compliance at Microsoft' <https://www.microsoft.com/en-us/legal/compliance> accessed 11 February 2018.
[111] HP Corporate Ethics <http://www8.hp.com/us/en/hp-information/global-citizenship/governance/ethics.html> accessed 1 March 2018.
[112] Gibbs S, 'Google's AI is Being Used by US military Drone Programme' (*7 March 2018*) <https://www.theguardian.com/technology/2018/mar/07/google-ai-us-department-of-defense-military-drone-project-maven-tensorflow> accessed 21 March 2018.
[113] The letter of employee to Google's leadership. https://static01.nyt.com/files/2018/technology/googleletter.pdf accessed 1 May 2018.
[114] Google Code of Conduct<thttps://abc.xyz/investor/other/google-code-of-conduct.html> accessed 1 May 2018.

IBM is the first company to sign up with the EU DP code of conduct for CSPs, which was launched by European Commission in January 2017.[115] This EU DP code, which is in accordance with the GDPR aims to improve transparency and facilitate the understanding by cloud users of DP issues and how they are addressed by CSPs in order to build trust and confidence in the cloud[116] This code is a voluntary instrument, allowing a CSP to evaluate and demonstrate its adherence to the code's requirements, either through (1) self-evaluation and self-declaration of compliance, or (2) through third-party certification.[117] IBM's code of conduct provides general guidance for resolving a variety of legal and ethical issues, which meet all of the EU DP Code's requirements.[118]

Codes of conduct or ethics are seen as good practice of organisations used for managing and guiding employee behavior to avoid any potential damage that is driven by unethical behaviours.[119] It would help CSPs to demonstrate that they are honest, reliable and trustworthy with a view to building trust with users. Accordingly, a number of CSPs tend to set out their codes of conduct which demonstrate compliance with the GDPR (contain obligations for improving transparency and control, promoting accountability of CSPs and increasing the data security as discussed in section 1 in order to reduce main concerns of cloud users about an inadequate level of DP.

Moreover, they tend to provide mechanisms for the administration, oversight and enforcement in order to demonstrate their acknowledgement and assumption of responsibility for having in place appropriate policies and good practices that include correction and remediation for failures and misconduct.[120]

---

[115] IBM Among the First Companies to Sign Up EU Data Code of Conduct for Cloud Service Providers <https://www.ibm.com/blogs/policy/eu-cloud-code-of-conduct/> accessed 1 May 2018.
[116] Commission, Data Protection Code of Conduct for Cloud Infrastructure Service Providers (27 January 2017).
[117] ibid 1.
[118] IBM Business Conduct Guidelines <https://www.ibm.com/investor/att/pdf/BCG_English_Accessible_2018.pdf> accessed 1 May 2018.
[119] Turculet M, 'Ethical Issues Concerning Online Social Networks' (2014) 149 Procedia Soc Behav Sci 967.
[120] See generally in De Bruin B and Floridi L, 'The Ethics of Cloud Computing' (2017) 23 Sci Eng Ethics 32; Ko R, Lee B.S. and Pearson S, 'Towards Achieving Accountability, Auditability and Trust in Cloud Computing' in Abraham A and others (eds), *Advances in Computing and Communications*

Critique

How effective codes of conduct or ethics charters are in building trust in the cloud remains unclear. There are a number of ethical challenges raised by an increased usage of various kinds of cloud services.[121] The ethics set out by different CSPs may be based on different standard, and this would add vulnerability to the data of cloud users.[122]

Additionally, it is uncertain whether CSPs would adhere to ethical standards?, who should assess this? and how can their breach be enforced, especially given that ethics are internal documents?[123] In this case, internal oversight and enforcement mechanisms are sometimes provided for: for example, a code of conduct may have to be endorsed and reviewed by Board of Directors and the President of the organisation will manage the compliance programme, with the support of an officer and committee for monitoring and auditing compliance.[124] However, since it is an internal mechanism, cloud users may not be sure that CSPs would take reasonable care to maintain their codes of conducts or ethics.

2.3 Increasing Data Security

This section will propose two possible approaches for preserving the confidentiality, availability and integrity of data residing in the cloud as follows:

2.3.1 Technical Approaches

Data security is always ranked among the issues that are of most concern to cloud users and the issues around data security do seem to have a huge impact on user trust in cloud computing. Thus, a technical approach is always seen as the critical approach for preserving data security in an online environment. This kind of approach could be used

---

(Communications in Computer and Information Science, vol 193. Springer, Berlin, Heidelberg 2011) 436-7.

[121] ibid 434-5.

[122] See generally in Timmermans J and Ikonen V, *The Ethics of Cloud Computing: A Conceptual Review* (Cloud Computing, Second International Conference, CloudCom 2010, November 30 - December 3, 2010, Indianapolis, Indiana, USA).

[123] Trope RL and Hughes SJ, 'Red Skies in the Morning - Professional Ethics at the Dawn of Cloud Computing' (2011) 38 Wm Mitchell L Rev 111, 250.

[124] McKendall M, DeMarr B and Jones-Rikker C, 'Ethical Compliance Programs and Corporate Illegality: Testing the Assumptions of the Corporate Sentencing Guidelines' (2002) 37 J Bus Ethics 367, 379.

by both cloud users and CSPs to protect the data against the intrusion of any third parties, including LEAs and NIAs.[125]

Following Edward Snowden's revelations, cryptography, which involves technical measures based on mathematical techniques in which the data will be applied by means of an algorithm for transforming the data into another language which cannot be understood by other people, has been considered to provide the best solution against the intrusion in our lives that the NSA and other state agencies in the world are pursuing.[126] Even though the cryptographic techniques can be used to strengthen the security of data residing in the cloud, their major disadvantage is that we cannot perform processing on the encrypted data, thus excluding most normal uses of the cloud except for basic storage.[127]

Thus, if data needs to be decrypted whenever it is to be processed, cloud users will have to provide the key to CSPs. This may affect the confidentiality and security of data stored in the cloud because the key may be shared with third parties. Again, this may be vital to the provision of a service by a sub-processor and thus may be an intrinsic part of customer needs.

One solution proposed to this, but only currently at the research level, is the idea of homomorphic encryption. This is a form of encryption which allows specific types of computations to be carried out on ciphertexts and to generate an encrypted result which, when decrypted, matches the result of operations performed on the plaintexts.[128] Homomorphic encryption allows CSPs to perform meaningful computations on encrypted data without knowing the private key (i.e. without decryption), so that the

[125] There may be various technical approaches, such as intrusion detection systems and firewalls, which could be used to preserve the security of data held in the cloud. However, due to the word limit, this section will only discuss some technical approaches in order to give an idea of how the technical approaches play a critical role in building users' trust in cloud computing.

[126] Kamara S and Lauter K, 'Cryptographic Cloud Storage' in Sion R and others (eds), *Financial Cryptography and Data Security: FC2010 Workshops Spain, January 2010* (Springer 2010).

[127] ENISA, Study on the Use of Cryptographic Techniques in Europe (20 April 2012); Zhou L, Varadharajan V and Hitchens M, 'Secure Administration of Cryptographic Role-Based Access Control for Large-Scale Cloud Storage Systems' (2014) 80 JCSS 1518.

[128] Iram A and Khandekar A, 'Homomorphic Encryption Method Applied to Cloud Computing' (2014) 4 IJICT 1519, 1522.

cloud user will be the only holder of the secret key.[129] Nevertheless, the question remains whether homomorphic encryption is efficient enough to be practical.[130] This is because fully homomorphic encryption can cause the system to run too slowly for practical use, so that this technique still needs to be improved if it is to be of commercial use.[131]

Another interesting approach is access control, which is mainly about a procedure that allows, denies or restricts access to the data and the system.[132] In access control systems, many steps, e.g. identification, authentication, authorisation and accountability have to be taken before actually obtaining access to the data. There are various types of access control models, such as Mandatory Access Control (MAC), Discretionary Access Control (DAC) and Role Based Access Control (RAC).[133] However, there are some limitations of each of these models when applying them in the context of cloud computing, e.g. MAC, in which a central authority is in command of giving access decisions to a subject that requests access to data, is inflexible and difficult to implement and DAC, which grants the data subjects the ability to restrict access to their data based upon their identities or their membership of certain groups, is less secure and is difficult to run in terms of system maintenance and verification.[134]

The best way to increase the security of data held in the cloud in this case would be to select the technical approach which is most appropriate for each particular context, e.g. for data stored in the server or for data processed between servers located in different locations.

---

[129] TEBAA M and HAJII SE, 'Secure Cloud Computing through Homomorphic Encryption' (2013) 5 IJACT 2013, 33; Poteya MM, Dhoteb CA and Sharmac DH, 'Homomorphic Encryption for Security of Cloud Data' (2016) 79 Procedia Comput Sci 175, 176.

[130] Lauter K, Naehrig M and Vaikuntanathan V, *Can Homomorphic Encryption be Practical?* (In Proceeding ACM Cloud Computing Security Workshop, 2011, page 113-124).

[131] Hayward R and Chiang C-C, 'Parallelizing Fully Homomorphic Encryption for a Cloud Environment' (2015) 13 J Appl Res Technol 245, 251: Bajpai S and Srivastava P, 'A Fully Homomorphic Encryption Implementation on Cloud Computing' (2014) 4 IJICT 811, 815.

[132] Gollmann D, 'Access Control in and around the Browser' in Huang X and Zhou J (eds), Information Security Practice and Experience: 10th International Conference, ISPEC 2014 Fuzhou, China, May 5–8, 2014 (Springer) 1-3.

[133] Onankunju BK, 'Access Control in Cloud Computing' (2013) 3 IJSRP 1, 1.

[134] Mulimani M and Rachh R, 'Analysis of Access Control Methods in Cloud Computing' (2017) 3 IJEME 15, 22. See generally in Younis YA, Kifayat K and Merabti M, 'An Access Control Model for Cloud Computing' (2014) 19 JISA 45.

2.3.2 Localised Cloud Computing

In chapter 4, I discussed at length the problem of trust for users that have data stored in the cloud, especially in the US, which may be accessed by foreign governments. The EU cloud users are concerned that when their data is stored in third countries, the data may not be protected at the same level as that provided by the EU DP law. One obvious solution to this is to restrict the data location to those countries that can provide an adequate level of DP to cloud users. This would also ensure, for EU cloud users, that their data will be subject to the law of countries that provide an adequate level of DP. There are two approaches which try to do this: firstly, a quite well known idea is that data should be stored by CSPs on servers that are local to the user; secondly, there is a much more recent and novel idea, that users should control their own data using what is sometimes known as a "Personal Data Container" (PDC).

The first approach is an attempt to keep users' data within a certain region, e.g. the EU.[135] This would be beneficial not only to EU cloud users, but also to local and regional CSPs, e.g. OVH, which is a popular French cloud computing company which provides many kinds of cloud service to users, e.g. private cloud and public cloud, as the market opportunities for them will be strong.[136] One example can be seen in the project of the German Federal Cloud "Bundescloud" in which Germany requires government cloud services to store personal data only in Germany and also requires government offices to use only cloud services that are certified by the government's IT security office, or equally strict standards.[137]

The second approach is for users to store and process their own personal data within a PDC. Conventionally, once cloud users have put their data in the cloud, they can only exercise control over their data to the extent that CSPs allow them to do so. Encrypting the data is not a practical approach, as has been mentioned above. Accordingly, the concept of the PDC that allows users to retain the ownership of their

[135] Singh J and others, *Regional Clouds: Technical Considerations* (Technical Report Number 863, November 2014) 18.
[136] Buest R and Miller P, *The State of Europe's Homegrown Cloud Market* (GIGAOM Research, A Cloud Report, 17 Sept 2013) 19; See more details at <https://www.ovh.com/world/> accessed 1 March 2018.
[137] See more details at <https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2015/05/it-konsolidierung.html> accessed 1 March 2018.

data and at the same time provides access to third parties on their own terms, might be an answer to the problem of the lack of secure control over data processing for users.[138]

History and Examples of Personal Data Container

The Databox project has been carried out since 2016 by scholars from Imperial College London, the University of Cambridge and the University of Nottingham.[139] The Databox concept posits a physical device as a gateway to a distributed platform and it is predicated on the "Dataware model", which implicates users (by or about whom data is created), data sources (e.g. connected devices, which generate data), a personal container (which collates the data produced by the data sources), a catalogue (which allows users to manage access to their personal containers), and data processors (external machines exploited by data controllers who wish to make use of the data).[140]

The Databox gathers data from local and remote sources, from online social networks to establish the heart of an individual's personal data processing ecosystem by providing a platform for managing secure access to data and enabling authorised third parties to provide an individual with authenticated services, including services that may be accessed while roaming outside the home environment. It envisions an open-source personal networked device that collates, curates and mediates specific, limited, logged access to an individual's personal data by verified and audited third party applications and services.[141]

Additionally, the Hub of All Things (HAT) Data Exchange Ltd, which runs a for-profit data exchange, also adopts the concept of a PDC.[142] HAT provides individuals

[138] Papadopoulou E, Taylor N and Williams H, *Enabling Data Subjects to Remain Data Owners* (In Agent and Multi-Agent Systems: Technologies and Applications, pages 239- 248 Springer, 2015).
[139] The Databox project is funded by the Engineering and Physical Science Research Council (EPSRC) and it is supported by the Internet Society and Cornell Tech and the Horizon Digital Economy Research Institute. This project runs from October 2016 to September 2019. See <https://www.databoxproject.uk/about/> accessed 11 January 2018.
[140] McAuley D, Mortier R and Goulding J, *The Dataware Manifesto* (Proceedings of the 3rd International Conference on Communication Systems and Networks, pp 1-6, Bangalore, IEEE, 2011).
[141] Mortier R and others, *Personal Data Management with the Databox: What's Inside the Box?* (Proceedings of the 2016 ACM Workshop on Cloud-Assisted Networking: December 12, 2016, Irvine, CA, USA) 49.
[142] See < https://hubofallthings.com/c/technology > accessed 11 January 2018.

with their own database (the Data Hub) which is capable of performing computations over data with a view to preserving the individual's privacy. This technology makes it possible for any app, service or website to be built in a way that gives individuals control over their own data, so that users can store, exchange and transact data privately.

Critique

The data subjects who use PDC are able to take a full control over their data and to engage directly in data transactions. They can determine what data should be shared and with whom they should be shared. This would remove the legal, economic and reputational risks in relation to the relevant regulations (e.g. GDPR).[143] However, the problem with this model is in cases where the service is only paid by the users (the data subjects) – as with Facebook's users, so there are no incentive to cooperate with PDC technologies. This is partly why these technologies are so slow in getting going. Databox has no actual working partnerships with commercial services as yet. HAT has been working with local transport companies.

Moreover, the personal data container is not a general approach which could be used by all cloud users to secure their data.[144] For many individual users, using a PDC will be technically challenging when compared to the easy interfaces of typical cloud services, e.g. Facebook, Gmail or GoCompare. It can be said that the concept of Databox is still at an early stage; there is an open challenge about how to afford users the possibility of finding personal equilibria with the sharing and use of their data.

CONCLUSIONS

The two legal problems in relation to the cloud which I discussed in chapters 3 and 4 have brought about a number of legal uncertainties which potentially reduce users' trust in cloud computing. That trust, as I established in chapter 2, is based on transparency and control, accountability and security. All of these are threatened by the problems outlined in chapters 3 and 4.

[143] ibid 13.
[144] Mortier R and others (n141) 50.

In this chapter, I have looked for solutions, including both legal and non-legal solutions, to these problems. Various ways have been canvassed to provide more transparency about the data residing in the cloud; to improve the ability of data subjects to exercise control over their data; to foster greater accountability; and to increase their data security.

In terms of legal solutions, which are mainly drawn from the GDPR, there are many approaches that could be used to achieve all these three criteria. In order to increase transparency, the GDPR sets out many transparency obligations, e.g. requiring that personal data should be processed lawfully, fairly and in a transparent manner, controllers must take appropriate measures to provide certain minimum information to data subjects, regarding the collection and further processing of their personal data in a concise, transparent, intelligible and easily accessible form, using clear and plain language.[145] The GDPR also supports the ability of cloud users to exercise control over their data by providing a range of rights to data subjects, e.g. the right of access to their data and to object to the data processing.[146]

In order to improve the accountability of CSPs, the GDPR introduces an accountability principle, which obliges controllers to be responsible for and to be able to demonstrate compliance with the GDPR.[147] It also sets out a mechanism to help controllers and processors to ensure their compliance and to allow data subjects to quickly assess the level of DP, e.g. codes of conduct, DP certification, DP seals and Data Protection Impact Assessment.[148] Additionally, the GDPR provides the data subjects with both judicial and non-judicial remedies against controllers, processors and supervisory authorities for all infringements.[149]

In order to increase data security, the GDPR sets out security obligations that require both the controller and the processor to implement appropriate technical and

[145] GDPR, Art 5(1),12-14, 15 -22 and 34.
[146] GDPR, Art 15-18 and 20-22.
[147] GDPR, Art 5(2).
[148] GDPR, Art 35-36, 40-41 and 42-43.
[149] GDPR, Art 77-84.

organisational measures to ensure a level of security appropriate to the risks, e.g. the pseudonymisation and the encryption of personal data.[150]

In terms of non-legal solutions, icons and labels could be used to increase *transparency* in addition to written policies communicating complex factual and legal matters to cloud users, but adopting icons and labels is not without problems, e.g. icons and labels may not be known and trusted by both users and CSPs and information may be too complex to be understood at a single glance. Similarly, transparency reports may allow users to make meaningful comparisons across providers which may then help them make an informed decision about their options, especially in relation to fears of access to their data by domestic or foreign governments. However, transparency reports, in no way provide a complete solution to build users' trust in the cloud since they do not empower cloud users to exercise full control over their data.

Transparency reports, alongside third party certification and trustmarks, which could be used to demonstrate to cloud users that CSPs take their privacy seriously and that they are willing to mitigate risks, monitor and identify risks and policy violations, manage incidents and provide redress, may also improve *accountability* and thus trust. Nevertheless, there are many challenges that seem to prevent these mechanisms from working satisfactorily to build trust in cloud computing, e.g. lack of oversight of self-regulatory trust mark schemes and the multiplicity of trust marks. Internal codes of ethics may do something of the same nature although they lack the element of external validation.

Finally, users themselves can take steps to protect the *security* of their data and thus increase their trust. This is akin to the way that some users already routinely encrypt their data before entrusting their data to CSPs. Providing a local cloud service may be a good way to make users feel that their data, especially high-stakes data held by the state such as tax, health or welfare data, will be adequately protected. A PCD is a useful approach for preserving the security of data, while retaining full control over it.

As trust in the cloud is a highly subjective matter that varies among different people and different contexts and there are obvious severe limitations in deploying each

[150] GDPR, Art 32.

of these approaches for enhancing trust in cloud computing, in the short term, none of them seem to offer an adequate solution to meet the challenge of improving user trust in the cloud. Adopting only either legal solutions or non-legal solutions does not seem to be powerful enough to encourage individuals and SMEs to be confident in entrusting their data with CSPs.

In order to achieve all three criteria for creating trust in cloud computing, adopting many different approaches would be likely to increase the possibility of individuals and SMEs placing their trust in cloud computing. For example, to invest in promoting technology like PDC and also pass laws to support them for improving data security, may be helpful in building trust in cloud computing, which could then potentially facilitate the use of cloud computing.

All these approaches would be very helpful for my home country of Thailand, which is the funder of my study, which (1) does not yet have practical regulation regarding the use of personal data in the cloud for protecting individuals' privacy or (2) is using or potentially supplying cloud services and which still does not have an appropriate approach to ensure that CSPs will provide trustworthy services. The legal solutions would be useful as a role model for passing Thai laws for governing the data processing in the cloud, in which the laws in this field have not yet been passed in Thailand. The non-legal solutions, would also provide a clear understanding of what can make cloud computing trustworthy to Thai CSPs and would provide useful information which would enable Thai cloud users to consider which CSPs they should entrust with their personal data. Especially, the concept of third party certification and technical approaches have always received huge attention from Thai society, as these could potentially help build trust in online services, certification, trust marks, trust seals are likely to be popular in Thailand where there is no specific DP law.

It should be noted that the problems about trust in cloud computing may no longer matter that much, especially in the non-competitive market or in the case of free services, like mail services (Yahoo or Gmail), since there is some empirical evidences showing that since Snowden users have continued to use the cloud in ever greater

numbers.[151] Accordingly, the question remains in some cases whether trust is being developed by a rational cause or whether it can be trumped by convenience and cost.

[151] See < https://www.rightscale.com/blog/cloud-industry-insights/cloud-computing-trends-2017-state-cloud-survey> and < https://www.rightscale.com/blog/cloud-industry-insights/cloud-computing-trends-2018-state-cloud-survey> accessed 1 July 2018.

CONCLUSIONS

Over the past few years, cloud computing has become a popular online service among various kinds of users, ranging from private to public sectors. However, the features of cloud computing do create a range of difficulties that prevent the existing legal frameworks from working effectively to preserve the privacy of data subjects. This situation seems to be having an impact on user trust in cloud computing, at least to some extent, as it does make users feel reluctant about adopting cloud computing.

This thesis aims to provide an analysis of how user trust in cloud computing is being disrupted by the two legal problems related to DP, which are the legal problems resulting from the application of the EU DP law in cloud computing and the legal problems regarding the EU and the US legal frameworks governing access to personal data held in cloud computing by LEAs and NIAs. The emphasis is on the trust of EU individuals and SMEs (who are too small to have their own facilities) as cloud users who entrust their data to CSPs, most of whom are US- based companies or have their data centres located within the US. Finally, two type of possible approaches (legal and non-legal) for building user trust in cloud computing, which has been damaged by these two legal problems, are proposed.

1. ANSWERS TO THE MAIN RESEARCH QUESTIONS

1.1 What is Cloud Computing?

Due to there being no common definition of cloud computing, Chapter 1 addresses this research question by examining the existing literatures from technological, business and legal perspectives and finally provides a description of cloud computing as

> *a paradigm for delivering IT capabilities over the Internet. It provides many kinds of services, ranging from merely software to the whole infrastructure in different models. Cloud resources are pooled together, so that cloud services are scalable and can be rapidly provisioned. It allows users to monitor and customise their own resources as needed. Cloud users will then be billed on the basis of their measured usage*.

Cloud computing can provide many kinds of services. It is commonly categorised by using a service model and a deployment model. There are three types of cloud service models: (1) *SaaS* provides software applications installed on CSPs' infrastructure; (2) *PaaS* provides a platform for developing, hosting and deploying software applications; and (3) *IaaS* provides a raw IT infrastructure, including computing, storage and networks. There are four types of cloud deployment models: (1) *Private cloud* is only available to one user; (2) *Public cloud* is available to all users; (3) *Community cloud* is operated for a specific community of users that share the same concerns, such as mission, policy and security requirements; and (4) *Hybrid cloud* is a combination of private, public and community clouds.

Despite the great number of benefits offered by cloud computing, such as reducing the cost of maintenance and increasing the flexibility of IT capabilities, its nature brings with it many risks to cloud users, such as risks associated with privacy and data security. Furthermore, legal scholars have raised the difficulties and challenges arising from the application of the existing laws in the cloud. The features of cloud computing are considered to be the main cause of preventing the existing laws in different fields, such as DP, contract, intellectual property and crime and forensic, from working effectively to achieve their objectives. This situation poses threats to the rights of cloud users, which could then potentially make them reluctant to adopt cloud computing.

1.2 What is Meant by Trust in Cloud Computing?

To answer this research question, Chapter 2 explores the relevant literatures from different disciplines, including psychology, sociology, business and electronic commerce, and finally concludes that trust in cloud computing is a strong expectation that comes into play to rationalise people's decisions to adopt cloud computing, which can present a variety of risks and uncertainties to cloud users, for the sake of taking the advantages of cloud computing.

Trust in cloud computing has received special attention from the public over the past few years, especially after the revelations of the PRISM scandal. Since then, many surveys have shown that individuals and SMEs are concerned about privacy and data security and this situation does seem to affect their trust in cloud computing, as they

have become hesitant about placing the data in the cloud. Furthermore, following the Cambridge Analytica revelation, the number of Facebook users in Europe is falling, resulting in the collapse of Facebook's share price by more than $119 in 2018.

Regarding all these situations, user trust in cloud computing does seem to be critical for cloud computing adoption, at lease to some extent. This is because cloud computing is clearly only viable if cloud users are willing to make themselves vulnerable by allowing their data to reside in the cloud, which they do not own, and allowing it to be controlled by the CSPs they have or other third parties, such as sub-CSPs, in spite of the fact that such providers may act in the ways that would have a negative impact on cloud users.

User trust in cloud computing does seem to depend on three main factors, which are (1) *transparency and control* – whether CSPs provide cloud users with enough information related to their data and whether cloud users can decide, track and audit how and where their data is being used, by whom and for what purposes; (2) *accountability* – whether CSPs take responsibility for the stewardship of personal data according to contractual and legal requirements and provide remedies for any damages resulting from their non-compliance; and (3) *data security* – whether CSPs employ necessary security measures for preserving the confidentiality, availability and integrity of data and to comply with cloud contracts and relevant legal obligations.

However, building user trust in cloud computing is not an easy task, as the best circumstance that can facilitate trust in cloud computing is considered to be a state of familiarity, which really needs history as a reliable background for absorbing the complexity, risk and uncertainty. Furthermore, once trust in cloud computing has been broken, it is quite difficult to rebuild. Accordingly, the most effective way to build trust in cloud computing is likely to lie in a combination of different kinds of approaches (for example a fair contract, trust marks and trust seals) that fulfill all of the above three factors.

1.3 How is User Trust in Cloud Computing Affected by the Legal Problems Regarding the Application of the EU DP Law to the Processing of Personal Data in Cloud Computing?

This research question has been addressed by Chapter 3, which provides a discussion of (1) the legal problems affecting trust in the cloud emerging from the application of the former EU DP law (DPD) to the processing of personal data in the cloud; and (2) whether the current EU DP law (GDPR) can address such problems.

There are three main legal problems, as discussed in Chapter 3, that affect user trust in cloud computing, because they all create legal uncertainties, which could then lead to the violation of the privacy rights of EU cloud users.

Firstly, identifying the controller and the processor, who is responsible for complying with the DP obligations imposed by the DPD, remains a perplexing matter. The DPD set out a rule for identifying the parties involved in the processing of personal data, which was based on the model of a binary division between those who controlled the means and purposes of processing and those who merely implemented those instructions.[1] This is not how cloud computing operates. The ability to exercise control over the processing of personal data in the cloud is divided between cloud users and CSPs, and which of them is the sole joint controller varies depending on the context. A sliding scale emerges in which some CSPs clearly exert more control over the ends and means of processing, while, in other scenarios, the user clearly remains the controller.

There are no changes made to the definition of a controller and a processor under the DPD by the GDPR, in order to help identify the status of cloud users and CSPs. It rather promotes the existing idea of a "joint controller" in the DPD and imposes greater obligations on processors.[2] This would not improve the existing situation, and may create more problems, such as requiring processors to obtain prior authorisation of the controller every time they engage with sub-processors, which is probably neither practical nor useful for preserving the security of data (Article 28(2)). Therefore, a whole new model that could assess the qualitative level of the control exercised by a particular CSP and could allocate either liability or immunity accordingly, might be considered a useful starting place for addressing the status and obligations of all the involved parties in the cloud.

[1] DPD, Art 2 (d)(e).
[2] DPD, Art 2 (d). And GDRP 26(1).

Secondly, it is not always easy to determine the territorial reach of the EU DP law and the applicable law in the cloud. Regarding Article 4 of the DPD, CSPs will be subject to the EU DP law under the circumstances where

(i) CSPs were established in the EU (EU CSPs) and the processing was carried out in the context of the activities of such an establishment;[3]

(ii) CSPs were not established in the EU (non-EU CSPs), but such CSPs were using equipment in the EU to process personal data.[4]

Once CSPs fall under the scope of the DPD, they have to comply with the DP law of the Member State where

(i) the establishment of the EU CSPs was located and the data processing was taking place in the context of the activities of such an establishment;[5]

(ii) the equipment used by non-EU CSPs for processing personal data was situated.[6]

In the case of the EU CSPs, it is unclear what is meant by the terms "establishment" and "in the context of the activities of an establishment".[7] Moreover, the implications of the courts' decisions, such as in case of *Google Spain,* are quite far-reaching and they lead to controversial points with regard to their extraterritorial effects.[8] Multinational CSPs would have to comply with multiple and potentially conflicting national DP laws.

In the case of non-EU CSPs, the DPD marked a significant extension of the extraterritorial application of the EU DP law. The "equipment" and "make use of equipment" grounds do catch a range of non-EU CSPs to be subject to the EU DP law, even if they do not know where the equipment they use for processing data is located.[9]

The GDPR does seem to reflect the nature of the cross-border processing of

[3] DPD, Art 4(1)(a).
[4] DPD, Art 4(1)(c).
[5] DPD, Art 4(1)(a).
[6] DPD, Art 4(1)(c).
[7] DPD, Art 4(1)(a).
[8] Case C–131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González, CJEU, Judgment of 13 May 2014.
[9] DPD, Art 4(1)(c).

personal data in the cloud more than the DPD did. In the case of the EU CSPs, it proposes a definition of the main establishment of the controller and the processor, which is relevant to the applicable law, rather than to the territorial scope. Thus, this could not address the question of territorial scope when the EU CSPs, who have more than one establishment, jointly determine the purposes of, and the means for, the personal data processing.[10] The law of the Member State where a data subject has his/her domicile seems to provide better grounds for applying the EU DP law to the EU CSPs and this would be more convenient for data subjects to enforce their rights against such CSPs. It also introduces a one stop shop rule that is used for identifying the leading DPA to deal with the situation where CSPs are subject to multiple and potentially conflicting rules of different nations' DP laws.[11] The applicable law would be the DP law of the jurisdiction of their leading DPA.

In the case of non-EU CSPs, the GPDR introduces the new and more precise connecting factors of "offering" and "monitoring", which, at first glance, seem to provide more certainty about the law that is applicable to personal data processing in the cloud.[12] Nevertheless, it rather brings a lot more non-EU CSPs within the territorial scope of the EU DP law, since any CSP is presumably "offering" its service within the EU.

Thirdly, it is quite difficult to apply the data export rules under the DPD, which restricts the location of the data transfer, in cloud computing, where the data transfer always involves multiple data centres located in different countries provided by many sub-CSPs (onward transfer).[13] Furthermore, the grounds for lawful transfer of personal data outside the EU, for example consent, SCCs, BCRs and Safe Harbor, did not work well in providing an adequate level of protection to personal data that had been transferred outside the EU.[14] The absence of a definition of "unambiguous consent" made it difficult to determine what constitutes valid consent under the DPD.[15] The SCCs

[10] GDPR, Art 4(16)(a) and (b).
[11] GDPR, Art 56.
[12] GDPR, Art 3 (2)(a) and (b).
[13] DPD, Art 25.
[14] DPD, Art 26.
[15] DPD, Art 4(h) and 26(1)(a).

and the BCRs were inflexible and did not cover all of the data transferring within the cloud. Regarding the PRISM scandal, the US-EU Safe Harbor Agreement was considered as not providing an adequate level of DP and was then ruled to be invalid in 2015.

The GDPR improves the current situation by extending the scope of the data export rule to cover the "onward transfer" of personal data from a non-EU country to another non-EU country.[16] This would cover more scenarios of data transfer within the cloud, but the problem remains as to how the EU data subjects enforce their rights against such non-EU data importers and exporters.

In the case of a lawful basis for data transfer, the GPDR replaces the notion of the "unambiguous" consent of the data subject in the DPD by the "explicit" consent, but definitions of these two types of consent are still absent; thus, the difficulties in obtaining meaningful consent from the data subjects still exist.[17] Moreover, consent would no longer be an option for data transfer within the cloud, as the GDPR does not allow the consent ground to be used for the massive and repetitive transfer of personal data that usually happens in the cloud.[18]

The GDPR has dealt with the inflexibility of the current SCCs by introducing two more types of such clauses, namely DPA clauses and ad hoc clauses.[19] This would allow non–EU CSPs to provide their services to EU data subjects, but who the DPA is in a non-EU country that is able to approve ad hoc clauses and cooperate with other DPAs in the Member State remains unanswered. BCRs for controllers and processors are, for the first time, formally recognised by the GDPR.[20] They would benefit CSPs, as they could be used for data processing in the cloud by sub-CSPs.

The Commission put in place the EU-US Privacy Shield, replacing the EU-US Safe Harbor Agreement, to improve the data transfer situation between the EU and the US. Although many improvements have been made by this Shield, it is subject to much

[16] GDPR, Rec 101 and Art 44.
[17] GDPR, Art 4(11) and 49(1)
[18] GDPR, Rec 111 and 113.
[19] GDPR, Art 46(2)(d)) and 46(3)(a).
[20] GDPR, Art 4(20) and 46.

criticism, as it cannot provide an adequate level of DP. This Shield and the SCCs are currently being challenged in many cases and have been referred to the CJEU to consider their validation. It remains to be seen what a valid legal basis for CSPs to transfer data outside the EU will be.

Possible solutions to all these problems would probably be to apply appropriate security measures, for example cloud users may encrypt their data before uploading it into the cloud and one way for the CSPs who want to deliver their services to EU cloud users might be to make it clear in the contract where their data will be stored or processed and what mechanism they will use to ensure a high level of DP regarding the EU DP law.

All these DP problems in the cloud seem to make individuals and SMEs hesitant about adopting cloud services, as they all violate the three critical factors for creating user trust in cloud computing: (1) *transparency and control* – these problems bring about a lot of legal uncertainties regarding how their data will be collected or processed, by whom and for what purposes and whether their data will be protected at the level required by the EU DP law, and this situation can make cloud users feel that they will lose control over their data; (2) *accountability* – these problems create a range of barriers that prevent CSPs from being responsible enough to comply with the obligations imposed by the EU DP law and to be liable to provide cloud users with remedies for any damages resulting from their actions; and (3) *data security* –these problems give rise to a variety of risks to the security of data residing in the cloud.

1.4 How is User Trust in Cloud Computing Affected by the Legal Problems Regarding the EU and US Legal Frameworks Governing Access to Personal Personal Data Held in Cloud Computing by Law Enforcement and National Intelligence Agencies?

The research question has been addressed by Chapter 4, which provides an analysis of the legal problems affecting trust in cloud computing emerging from the EU and US legal frameworks governing the access to personal data held in cloud computing by LEAs and NIAs. The emphasis is on the issue of the US LEAs and NIAs obtaining access to the personal data of EU cloud users.

Due to the fact that various different kinds of data reside in the cloud, ranging from general to confidential data, there is a high possibility that LEAs and NIAs will seek to obtain access to the data held in the cloud potentially relating to criminal activity in various different countries for the sake of preventing, investigating, detecting and prosecuting crimes and acts of terrorism. The US NSA PRISM and related programs have been attracting special attention with regard to the fact that the activities of public agencies in obtaining access to personal data entrusted with CSPs may be violating the privacy rights of EU data subjects, even when, in some cases, such access has been authorised by US laws.

The problems regarding US laws and the EU-US agreements that allow the US agencies to obtain access to the data of EU cloud users are the main causes that lead to the violation of privacy rights of EU data subjects. Firstly, defects in US legal instruments lead to mass surveillance. Traditionally, the Convention on Cybercrime and the MLAs application are the main legal and formal approaches that allow the US LEAs to acquire the personal data of EU data subjects (foreign data) for law enforcement purposes, but they do not seem to be working effectively to protect the privacy of EU data subjects.[21] The Convention on Cybercrime has been considered to be a symbolic policy and to have only a limited effect on combating cybercrime. In the US, this Convention has provoked many controversial issues, especially the lack of adequate privacy protection provided by this Convention and the unjustified expansion of investigative powers. Moreover, MLATs in practice have been subject to many problems, e.g. their procedure can be costly, slow and cumbersome.

Accordingly, it is observable that agencies may feel constrained to turn to other less globally acceptable routes or sometimes to illegal routes to obtain access to personal data held in the private sector. They may choose to make a direct request to the US CSPs to obtain access to such data, or, somewhat less legally, they may launch a "back door search" to a cloud server located within or outside the US for law enforcement and national security purposes.

[21] The Convention on Cybercrime, CETS. 185, Budapest, 23 November 2001, Treaty Series No. 18 (2012); Mutual Legal Assistance; Agreement Between the United States of America and the European Union, Signed at Washington June 25, 2003.

Secondly, although there are a number of US laws for protecting the privacy of EU cloud users when the public agencies gain access to their data for law enforcement and national security purposes, they do not provide sufficient privacy protection to EU cloud users. This is because there are differences in the expectations of legal protection and the legal regimes around privacy protection in the US and the EU. While privacy is recognised as a human right in Europe, which applies to all individuals, regardless of their identity, in the US there is no concept of privacy rights as human rights equivalent to the one that is entrenched in the EU laws.[22] There is only the concept of privacy rights as civil rights of US persons, in which the Fourth Amendment of the US Constitution provides protection only to US persons. Moreover, in the EU, there are comprehensive legal frameworks on privacy protection with regard to the processing of personal data within both private and public sectors. In contrast, in the US, there is no such single and comprehensive legal framework and the privacy protection guarantees are in general sector-specific.

Apart from that, the US laws lag significantly behind in granting equal rights to US and EU citizens. The US laws that cause considerable anxiety regarding the privacy of EU data subjects are the FISA of 1978, the USA Patriot Act of 2001 and the FISAA of 2008, which contain provisions which allow for discrimination between US and non-US persons. The requirements imposed by such legal frameworks for carrying out electronic surveillance on US persons do seem to be higher than those for non-US persons.

Even though, following the Snowden revelations of the US NSA mass surveillance programme in 2013, the US has proposed many legal instruments to address the problems with the US laws with a view to building trust between the EU and the US, they do not all work satisfactorily to achieve this aim. The Judicial Redress Act of 2015 creates new rights for EU data subjects to bring actions against US agencies under the Privacy Act of 1974, to obtain civil remedies for damage resulting from unlawful disclosure of their personal data and to obtain access to and correct government records

[22] The Convention for the Protection of Human Rights and Fundamental Freedom, Rome 1950 (European Convention on Human Rights, as amended), 1 June 2010.

about themselves, but this Act is subject to many limitations and exceptions that prevent EU data subjects from exercising their rights.

The USA Freedom Act of 2015 aims to end the ability of the US agencies to collect telephone metadata in bulk under section 215 of the USA Patriot Act and to provide a program that requires the agency to conduct searches in a more targeted manner, but it does not go far enough to curtail the agency's mass surveillance of non-US communications.

The US Liberty Act of 2017, the US Rights Act of 2017 and the FISA Amendment Reauthorisation Act of 2017, have been passed to reauthorise and reform section 702 of FISA, in order to strengthen the protection of individual privacy. But they mostly protect US citizens rather than EU citizens. The Cloud Act of 2018 enables agreements between the US and non-US governments, whose agencies are permitted by this Act to directly request data from US service providers, so that those agencies can bypass the legal safeguards of the MLATs regime and they can circumvent national privacy laws in Europe and elsewhere. This situation tends to pose a new threat to the privacy of both US and non-US persons.

Apart from that, the EU-US Privacy Shield, (now replaces the Safe Harbor Agreement), has been negotiated for cross-border transfers of personal data from the EU to the US in order to ensure that the level of privacy protection provided to EU data subjects will be essentially equivalent to that provided under the EU law. Nevertheless, it faces challenges in many cases, as it does not provide sufficient protection for personal data that is transferred from the EU to the US.

Additionally, there is the EU-US umbrella agreement, which establishes a minimum level of privacy protection regarding data exchanges for the purposes of the prevention, detection, investigation and prosecution of criminal offences, including terrorism, by providing safeguards and guarantees of lawfulness for data transfers as required by EU laws. However, this agreement in many respects fails to meet important substantive requirements of EU DP law. Some clarification is still needed in order to ensure that the level of protection of personal data afforded by the Umbrella Agreement is fully consistent with the EU law.

As a result of all these problems, it can be concluded that the relevant US laws and the EU-US agreement permitting the US agencies to obtain access to the personal data of EU cloud users for law enforcement and national security purposes do not meet the international standards (the ECHR), and the EU standards (like the EU Charter), which is what the EU cloud users expect when they entrust their data to US CSPs. There is no adequate level of privacy protection provided to the EU cloud users.

Regarding the empirical evidence provided in chapter 2, section 2.2, all these circumstances do seem to be affecting the trust of EU cloud users, at least to some extent. This is because the three factors creating trust in the cloud seem to be disrupted by these problems, which means that this situation could potentially make individuals and SMEs reluctant to adopt cloud services. Firstly, with regard to (1) *transparency and control* - these problems give rise to a number of issues of uncertainty with regard to the status of the data after it is entrusted to CSPs, and this situation tends to prevent cloud users from deciding, tracking and auditing how and where their data is being used, by whom and for what purposes; with regard to (2) *accountability* - these problems create challenges for CSPs to take responsibility for the stewardship of the personal data of cloud users according to their contractual and legal requirements due to the fact that US agencies may launch a backdoor access to the data, without the acknowledgement of the CSPs and data subjects; and with regard to (3) *data security* - these problems make it difficult to preserve the confidentiality, availability and integrity of data, since CSPs may be forced by US laws to allow US agencies to obtain access to the data of EU cloud users and this situation would then pose some threats to the security of the data of cloud users.

1.5 What are the Possible Approaches for Building User Trust in Cloud Computing?

An attempt has been made in chapter 5 to provide an analysis of the possible solutions to the lack of trust in cloud computing, which is affected by the two legal problems with DP as discussed in chapters 3 and 4. Chapter 5 proposes two main types of solution for building user trust in cloud computing, including legal and non-legal solutions, which aim at achieving the three main factors for creating trust in cloud computing, including

(1) rights to transparency and control of personal data; (2) accountability of CSPs; and (3) security of data placed in the cloud.

The legal solutions focus on approaches which are only drawn from the GDPR. The GDPR sets out a range of obligations to enhance transparency and improve the ability of cloud users to exercise control over their data. The transparency principle is a critical principle in the GPDR which requires that when ensuring that personal data are processed lawfully, fairly and in a transparent manner, controllers must take appropriate measures to provide certain minimum information to data subjects, regarding the collection and further processing of their personal data in a concise, transparent, intelligible and easily accessible form, using clear and plain language.[23] The GDPR supports the ability of cloud users to exercise control over their data by providing a number of rights to data subjects, e.g. the right to access to data, to erasure and to object to the data processing.[24]

In order to strengthen the accountability of CSPs, the GDPR introduces an accountability principle, which obliges controllers to be responsible for, and to be able to demonstrate compliance with, the GDPR.[25] It also sets out a mechanism to help controllers and processors to ensure their compliance and to allow data subjects to quickly assess the level of DP, e.g. codes of conduct, DP certification, DP seals and Data Protection Impact Assessment.[26] Moreover, it provides many approaches to get judicial and non-judicial remedy, i.e. the right to an effective judicial remedy against a supervisory authority, a controller or processor and the right to compensation and liability.[27]

In order to increase data security, the GDPR sets out security principles requiring both the controller and the processor to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, e.g. the pseudonymisation and encryption of personal data.[28] Moreover, it requires the controller,

[23] GDPR, Art 5(1),12-14, 15 -22 and 34.
[24] GDPR, Art 15-18 and 20-22.
[25] GDPR, Art 5(2).
[26] GDPR, Art 77-84.
[27] GDPR, Art 77-84.
[28] GDPR, Art 32.

without undue delay, to notify personal data breaches to the competent supervisory authority, no later than 72 hours after having become aware of it and it also requires the processor to notify such data breach to the controller without undue delay.[29]

The non-legal solutions are proposed as additional mechanisms to help increase the possibility of individuals and SMEs placing their trust in cloud computing as follows:

Firstly, labels and icons are considered to be helpful in the cloud for enhancing *transparency* about the data held in the cloud and then improving user awareness and comprehension of complex factual or legal matters with regard to what is happening with their data, as stated in privacy policies, which normally could not be easily understood. Ideally, icons should be clear, simple and well-designed in order to be able to convey information by means of one single graphic representation expressing the relevant content in an understandable manner for wide audiences, ideally even across different cultures.

Compared with icons, labels indicate more specific information about cloud services. They could be used to simplify privacy policies that are often confusing due to e.g. the use of specific or legal terms. This notion has become popular in the form of labels on food packaging, or energy rating, which have gained widespread recognition around the world, as they enable users to understand and comprehend the privacy policies more easily and make accurate privacy assessments.

However, building user trust in cloud computing by using icons and labels is not an easy task. First, icons and labels may not be known and trusted by both users and CSPs because there are a variety of icons and labels representing privacy options, which will differ across service providers. Therefore, standardisation of icons and labels and a consistent representation language that can facilitate machine to machine interoperability are needed. Second, information may be too complex to understand at a single glance, so that there should be a single page hand-out providing the meaning of the icons and describing useful terms. Third, labels may either sacrifice too much or too little information at once for users. Finding a balance in the amount of information provided

[29] GDPR, Art 33.

on the labels is thus required to improve the understanding of users. Last, icons and labels may not actually be properly deployed by CSPs and the use of icons and labels differs across various service providers and is subject to self-regulatory schemes. Accordingly, there should be an independent Ombudsman and sanctions when the providers fail to implement icons clearly and accurately.

Secondly, transparency reports are documents disclosing a variety of statistics about matters such as requests for content removal or blocking and governmental requests for access to user data. These reports could improve *transparency* by (1) allowing users to find out if a government or any third party is accessing their data held in the cloud and thus to alert them to government abuse; (2) holding CSPs to account when they allow covert state access to user data; (3) monitoring the performance of CSPs comparatively which can help users make informed choices.

Nevertheless, how effective these transparency reports are in practice remains uncertain because these reports are not required by the law and are designed by different CSPs, so that the quality of these reports provided by various CSPs seem to be inconsistent. There should be transparency reporting standards requiring CSPs to notify impacted users of information about requests made by LEAs and NIAs. Additionally, there should be guidelines or common practice on how CSPs deal with such requests in order to enable users to be sure that their data will be protected with an adequate level of protection, as demanded by the relevant regulations, and to prevent CSPs from quietly changing an internal practice in the future in response to government requests. However, transparency reports are in no way a completes solution to build and restore trust in the cloud since this reports merely disclose; they do not give users remedies. It does not empower cloud users to have full control over their data.

Thirdly, certification, trust marks and trust seals could be used to strengthen the *accountability* of CSPs. So-called Trustmark Organisations (TMOs) are typically independent third parties that provide a trust mark or trust seal to reassure users that CSPs to which they award such certification are in compliance with the TMO's standards. These three mechanisms will demonstrate to cloud users that CSPs take their privacy seriously and that they are willing to invest in DP, so that they will mitigate

risks, monitor and identify risks and policy violations, manage incidents and provide redress. Nevertheless, there are many challenges that seem to prevent these mechanisms from working satisfactorily to build trust in cloud computing, i.e. lack of oversight of self-regulatory trust mark schemes and multiplicity of trust marks.

Accordingly, a set of minimum criteria to harmonise all national trust marks may help improve the current situation. Moreover, it is worth setting up a uniform practice/code of conduct of TMOs to (1) require CSPs to give their users appropriate control and transparency over the data processing; (2) reassure users that their data will be processed in accordance with a code of conduct; and (3) monitor and confirm the consistent compliance of CSPs with users' expectations and the relevant regulations; and (4) signal the dependability and trustworthiness of CSPs to users.

Fourthly, internal codes of conduct or ethics may provide a possible approach for CSPs to instil user trust in cloud computing by engaging in internal audit, or publishing a list or code of ethical principles that they plan to adhere to, instead of asking for a third party certification. These would probably help enhance the *transparency* of how CSPs take care of their data and improve the *accountability* of CSPs, as they are able to demonstrate an acknowledgement of their responsibilities to comply with the commitments (based on contractual and relevant legal obligations) and to provide correction and remediation for failures and misconduct with a view to preserving the fundamental rights of cloud users.

This is easier and cheaper than using a third party body but it is arguably even more open to lack of true enforcement and being a matter of "something must be seen to be done" rather than a true solution. Additionally, ethics has a dynamic character and it varies across context and data location. It remains uncertain: (1) whether several CSPs adhere to the highest ethical and governance standards; (2) how to and who will enforce them when there is a violation?; and (3) is there any remedy for cloud users? Accordingly, a diverse and inclusive culture of internal codes of conduct or ethics should be built to serve as guidelines for CSPs and their employees to make good decisions and ethical choices in situations where there are conflicting interests. At the same time, strict administration and oversight of the compliance regime, and

enforcement and redress mechanisms, should also be established to ensure the effectiveness of the internal codes of conduct or ethics.

Fifthly, an appropriate technical approach is always considered the best approach for increasing the security of data, regardless of the data location and also to make it easier for CSPs to hold themselves accountable for their commitments. This could be used to protect the personal data from the intrusion of any third parties, including LEAs and NIAs. One of the most popular technique is cryptography, which is based on mathematical techniques in which the data will be applied by means of an algorithm for transforming the data into another language which cannot be understood by other people. But the fact that such encrypted data could not be processed, does prevent CSPs from doing their business because the power of the cloud can only be exploited when users are able to carry out computation on the data.

Due to the fact that the data needs to be decrypted whenever it is to be processed, cloud users will have to provide the key to CSPs. This situation may pose some risks to the confidentiality and security of data stored in the cloud because the keys may be accessible by any third parties. Homomorphic encryption thus would be the solution for this problem since it is a form of encryption which allows specific types of computations to be carried out on encrypted data. However, fully homomorphic encryption still needs to be improved since it can cause the system to run too slowly.

Another interesting approach is access control, which mainly employs a procedure that allows, denies or restricts access to the data and the system. However, there are some limitations of such access control models when applied to the cloud, e.g. Mandatory Access Control (MAC), in which a central authority is in command of giving access decisions to someone who requests access to data, is inflexible and difficult to implement. Therefore, the best way to increase the security of data held in the cloud would be to select the appropriate approach for each particular context, e.g. for data stored in the server or for data processed between servers located in different locations.

Lastly, localised cloud computing contains two different concepts which aim to increase the *security* of data residing in the cloud. The first is to restrict the data location within the country that can provide an adequate level of DP to cloud users. In response

to the PRISM scandal, CSPs may deal with privacy concerns of EU users by letting them choose the location where their data will be stored or processed. This approach provides CSPs with an opportunity to position themselves as fully transparent, trusted partners for assuring that the data will be kept within certain borders to build user trust in the cloud.

However, the data localisation is likely to have a dramatic impact on the ability of most of the well-known multinational CSP companies (which are normally headquartered in the US) to conduct business in the EU. This approach could only provide a short-term advantage to cloud users because the data location is no longer matters for security purposes in an online context, especially in the cloud, where the data can be processed and located anywhere around the world.

The second is the use of Personal Data Container, which provides an individual's personal data processing ecosystem that is capable of performing computations. This active platform allows an individual data subject to manage, log and audit access to their data by other parties. Users are able to determine what data should be shared and whom they should share their data with. This approach could help avoid risks of data breaches associated with collecting and curating large personal datasets which any third parties may have significant incentives to attack and steal.

But this concept is still at an early stage and there are controversial issues that need to be taken into account: (1) it is not a general approach for all users. The users need to be able to manage the use of their personal data, so that there should be instructions for adopting PDC provided to the users; and (2) the PDC is only paid by the users' data – as with Facebook's users, so Facebook has no incentive to cooperate with PDC technologies. This is partly why these technologies are so slow in getting going. Databox has no actual working partnerships with commercial services as yet. HAT has been working with local transport companies.

To conclude, trust is a highly subjective aspect that varies among different people and different contexts. There are also some limitations to employing several of the proposed approaches for enhancing trust in cloud computing, so that adopting one single approach may not be powerful enough to encourage individuals and SMEs to be

confident about entrusting their data with CSPs. Therefore, adopting many kinds of approaches in order to achieve all these three criteria would likely increase the possibility of individuals and SMEs placing their trust in cloud computing, which then could potentially facilitate faster use of cloud computing.

BIBLIOGRAPHY

Books

Anderson R J, *Security Engineering - A Guide to Building Dependable Distributed Systems* (2rd ed, John Wiley & Sons 2008).

Arasaratnam O, 'Introduction to Cloud Computing' in Halpart B (ed), *Auditing Cloud Computing: A Security and Privacy Guide* (John Wiley & Sons 2011).

Balboni P, *Trustmarks in E-Commerce: The Value of Web Seals and the Liability of Their Providers* (T.M.C Asser Press 2009).

Bateson P, 'The Biological Evolution of Cooperation and Trust' in Gambetta D (ed), *Trust : Making and Breaking Cooperative* (Basil Blackwell 1988).

Bauer E and Adams R, *Reliability and Availability of Cloud Computing* (John Wiley & Sons 2012).

Baun C and others, *Cloud Computing: Web-Based Dynamic IT Services* (Springer 2011).

Bernal P, *Internet Privacy Rights: Rights to Protect Autonomy* (CUP 2014).

Beyleveld D and Brownsword R, *Consent in the Law* (Hart Publishing 2007).

Bradbury JA, Branch KM and Focht W, 'Trust and Public Participation in Risk Policy Issues' in Cvetkovich G and Lofstedt RE (eds), *Social Trust and the Management of Risk* (Earthscan Publications Ltd 1999).

Bradshaw S, Millard C and Walden I, ‘Standard Contracts for Cloud Service’ in Millard C (ed), *Cloud Computing Law* (Oxford University Press 2013).

Brandeis L, *Other People's Money, and How Banker Use It* (Cosimo 2009).

Buyya R, Vecchiola C and Selvi ST, *Mastering Cloud Computing Foundations and Applications Programming* (Elsevier 2013).

Carnevale DG, *Trustworthy Government : Leadership and Management Strategies for Building Trust and High Performance* (Jossey-Bass 1995).

Castelfranchi C and Falcone R, *Trust Theory: A Socio-Cognitive and Computational Model* (John Wiley & Sons, Ltd., Publication 2010).

Chang H, ‘Data Protection Regulation and Cloud Computing’ in Cheung ASY and Weber RH (eds), *Privay and Legal Issues in the Cloud* (Edward Elgar Publishing Limited 2015).

Churchill W, ‘Cloud Computing Fundamentals’ in Krutz RL and Dean RV (eds), *Cloud Security: A Comprehensive Guide to Secure Cloud Computing* (John Wiley & Sons 2010).

Clarke K and others (eds), *Trust in Technology: A Socio-Technical Perspective*, vol 36 (Springer 2006).

Coleman JS, *Foundations of Social Theory* (Harvard University Press 1994).

Cuijpers C, Purtova N and Kosta E, ‘Data Protection Reform and the Internet: the Draft Data Protection Regulation’ in Savin A and Trzaskowski J (eds), *Research Handbook on EU Internet Law* (Edward Elgar 2014).

Cvetkovich G and Lofstedt ER, 'Conclusion: Social Trust, Consolidate and Future Advances' in Cvetkovich G and Lofstedt ER (eds), *Social Trust and Risk Management* (Earthscan Publication Ltd. 1999).

Dasgupta P, 'Trust as a Commodity ' in Gambetta D (ed), *Trust: Making and Breaking Cooperative Relations* (Basis Blackwell 1988).

De Bruin R, *Consumer Trust in Electronic Commerce: Time for Best Practice* (Kluwer Law International 2002).

DeGeorge RT, *Competing with Integrity in International Business* (OUP 1993).

Dixon M, *Textbook on International Law* (7 edn, OUP 2013).

Earle TC and Cvetkovich G, 'Social Trust and Culture in Risk Management' in Cvetkovich G and Lofstedt ER (eds), *Social Trust and the Management of Risks* (Earthscan Publications 1999).

Edward C, The Shorter Routledge Encyclopedia of Philosophy (Routledge 2005).

Edwards L, 'Privacy and Data Protection Online : The Laws Don't Work? ' in Edwards L and Waelde C (eds), *Law and the Internet* (3 edn, Hart Publishing 2009).

Edwards L, 'The Fall and Rise of Intermediary Liability Online' in Edwards L and Waelde C (eds), *Law and the Internet* (3 edn, Hart Publishing 2009).

Egger F, Consumer Trust in E-Commerce; From Psychology to Interaction Design' in Prins JEJ and others (eds), *Trust in Electronic Commerce : The Role of Trust from a Legal an Organisational and a Technical Point of View* (Kluwer Law International 2002).

Foster I and Kesselman C, ‘Concepts and Architecture’ in Foster I and Kesselman C (eds), *The Grid 2 : Blueprint for a New Computing Infrastructure* (Morgan Kaufmann Publishers 2003).

Fukuyama F, *Trust: The Social Virtues and the Creation of Prosperity* (Free Press 1995).

Furht B, ‘Cloud Computing Fundamentals’ in Furht B and Escalante A (eds), *Handbook of Cloud Computing* (Springer 2010).

Gambetta D, ‘Can We Trust Trust?’ in Gambetta D (ed), *Trust: Making and Breaking Cooperatives* (Basil Blackwell 1988).

——, ‘Foreward’ in Gambetta D (ed), *Trust: Making and Breaking Cooperative Relations* (Basil Blackwell 1988).

Good D, ‘Individuals, Interpersonal Relations, and Trust’ in Gambetta D (ed), *Trust: Making and Breaking Cooperative Relations* (Basil Blackwell 1988).

Hardin R, *Trust* (Polity Press 2006).

Hardstone G, Adderio Ld and Williams R, ‘Standardisation, Trust and Dependability’ in Clarke K and others (eds), *Trust in Technology : A Socio -Technical Perspective*, vol 36 (Springer 2006).

Hawthorn G, ‘Three Ironies in Trust’ in Gambetta D (ed), *Trust: Making and Breaking Coorperative Relations* (Basil Blackwell 1988).

Hill R and others, *Guide to Cloud Computing: Principles and Practice* (Springer 2013).

Hon WK and Millard C, ‘Cloud Technologies and Services’ in Millard C (ed), *Cloud Computing Law* (OUP 2013).

——, ‘Control, Security and Risks in the Cloud ’ in Millard C (ed), *Cloud Computing Law* (OUP 2013).

——, ‘How Do Restrictions on International Data Transfers Work in Clouds? ’ in Millard C (ed), *Cloud Computing Law* (OUP 2013).

Hon WK, Millard C and Walden I, ‘Negotiated Contracts for Cloud Services’ in Millard C (ed), *Cloud Computing Law* (OUP 2013).

——, ‘Who is Responsible for Personal Data in Clouds?’ in Millard C (ed), *Cloud Computing Law* (OUP 2013).

Hon WK, Hornle J and Millard C, ‘Which Law(s) Apply to Personal Data in Cloud ?’ in Millard C (ed), *Cloud Computing Law* (OUP 2013).

Hutchings A, Smith RG and James L, ‘Criminals in the Cloud: Crime, Security Threats, and Prevention Measures’ in Smith RG, Chung Cheung RC- and Chung Lau LY- (eds), *Cybercrime Risks and Responses* (Springer 2015).

Jin H and others, ‘Cloud Types and Services’ in Furht B and Armando E (eds), *Handbook of Cloud Computing* (Springer 2010).

Kamara S and Lauter K, ‘Cryptographic Cloud Storage’ in Sion R and others (eds), *Financial Cryptography and Data Security: FC2010 Workshops Spain, January 2010* (Springer 2010).

Kavis MJ, *Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS)* (Wiley 2014).

Kerkhof P and Van Noort G, 'Third Party Internet Seals - Reviewing the Effects on Online Consumer Trust' in Lee I (ed), *Encyclopedia of E-Business Development and Management in the Global Economy* (Hershey PA: Information Science Reference 2010).

Kosta E, *Consent in European Data Protection Law* (Martinus Nijhoff 2013).

Kuner C, *European Data Protection Law : Corporate Compliance and Regulation* (2 edn, OUP 2007).

——, *Binding Corporate Rules: Corporate Self-Regulation of Global Data Transfers* (OUP 2012).

Lane C, 'Introduction: Theories and Issues in the Study of Trust' in Lane C and Reinhard B (eds), *Trust Within and Between Organisations : Conceptual Issues and Empirical Applications* (OUP 2000).

Lau MW, *The Economic Structure of Trusts* (OUP 2011).

Lehmann A, Whitehouse D and Fischer-Hübner S (eds), *Privacy and Identity Management Facing up to Next Steps*, vol 128 (Springer 2017).

Leif-Erik Holtz, Harald Zwingelberg and Marit Hansen, 'Privacy Policy Icons' in Jan Camenisch, Simone Fischer-Hübner and Kai Rannenberg (eds), *Privacy and Identity Management for Life* (Springer 2011).

Luhmann N, *Trust and Power*, vol 3 (John Wiley & Sons Ltd 1979).

——, ‘Familiarity, Confidence, Trust: Problems and Alternatives’ in Gambetta D (ed), *Trust: Making and Breaking Co-operative Relations* (Wiley-Basil Blackwell 1988).

Mahmood Z, ‘Cloud Computing for Enterprise Architectures’ in Mahmood Z and Hill R (eds), *Cloud Computing for Enterprise Architectures* (Springer 2011).

Martin KM, *Everyday Cryptography: Fundamental Principles and Applications* (OUP 2012).

Matsuura JH, *Security, Rights and Liabilties in E-Commerce* (Artech House 2002).

McKnight DH, ‘Trust in Information Technology’ in Davis BG (ed), *The Blackwell Encyclopedia of Management Information System*, vol 7 (Wiley-Blackwell 2005).

Micek P and Aydin DD, ‘Non-Financial Disclosures in the Tech Sector: Furthering the Trend’ in Taddeo M and Floridi L (eds), *The Responsibilities of Online Service Providers*, Law Governance and Technology Series Volume 31 (Springer 2017).

Mollering G, *Trust: Reason, Routine, Reflexivity* (Elsevier 2006).

Noor TH, Sheng QZ and Bouguettaya A, *Trust Management in Cloud Services* (Springer 2014).

Parkhill D, *The Challenge of Computing Utility* (Addison-Wesley Pub 1966).

Pearson S, ‘Privacy, Security and Trust in Cloud Computing’ in Pearson S and Yee G (eds), *Privacy and Security for Cloud Computing* (Springer 2013).

Poullet Y and Dinan JM, 'The Internet and Private Life in Europe: Risks and Aspirations' in Kenyon AT and Richardson M (eds), *New Dimensions in Privacy Law* (CUP 2006).

Prins C and Van Der Wees L, 'E-Commerce and Trust : a Variety in Challenges' in Prins JEJ and others (eds), *Trust in Electronic Commerce : The Role of Trust from a Legal an Organisational and a Technical Point of View* (Kluwer Law International 2002).

Probst CW and others, 'Privacy Penetration Testing: How to Establish Trust in Your Cloud Provider' in Gutwirth S and others (eds), *European Data Protection: In Good Health?* (Springer 2012).

Quelle C, 'Not Just User Control in the General Data Protection Regulation On the Problems with Choice and Paternalism, and on the Point of Data Protection' in Shaw MN, *International Law* (7 edn, CUP 2014).

Rae AK, Hausen H-L and Robert P, Software Evaluation for Certification: Principles, Practice, and Legal Liability (McGraw-Hill 1995).

Ratnasingam P and Pavlou P, 'Technology Trust in Internet-based Interorganizational Electronic Commerce' in Khosrow-Pour M (ed), *The Social and Cognitive Impacts of E-Commerce on Modern Organizations* (Idea Group Publishing 2004).

Reed C and Cunningham A, 'Ownership of Information in Clouds' in Millard C (ed), *Cloud Computing Law* (OUP 2013).

Rountree D and Castrillo I, *The Basics of Cloud Computing: Understanding the Fundamentals of Cloud Computing in Theory and Practice* (Syngress 2013).

Roy J. Lewicki and Barbara Benedict Bunker, 'Developing and Maintaining Trust in Work Relationships' Trust in Organizations: Frontiers of Theory and Research, (SAGE Publications 1996).

Sabharwal N, *Cloud Capacity Management* (Apress 2013).

Sako M, 'Does Trust Improve Business Performance?' in Lane C and Bachmann R (eds), *Trust Within and Between Organisations: Concept Issues and Empirical Applications* (OUP 2000).

Schellekens M and Van Der Wees L, 'ADR and ODR in Electronic Commerce' in Prins JEJ and others (eds), *Trust in Electronic Commerce : The Role of Trust from a Legal an Organisational and a Technical Point of View* (Kluwer Law International 2002).

Shroff G, *Enterprise Cloud Computing : Technology, Architecture, Applications* (CUP 2013).

Simou S and others, 'Cloud Forensics: Identifying the Major Issues and Challenges' in Hutchings A, Smith RG and James L (eds), *Advanced Information Systems Engineering 26th International Conference, CAiSE 2014 Thessaloniki, Greece, June 16–20, 2014 Proceedings* (Springer 2014).

Slovic P, 'Perceived Risk, Trust and Democracy' in Cvetkovich G and E. Lofstedt R (eds), *Social Trust and the Management of Risk* (Routledge 1999).

Staiger DN, 'Cross-Border Data Flow in the Cloud Between the EU and the US' in Weber RH and Cheung ASY (eds), *Privacy and Legal Issues in Cloud Computing* (Edward Elgar Publishing 2015).

Stanoevska-Slabeva Katarina and Thomas W, ‘Cloud Basics - An Introduction to Cloud Computing’ in Stanoevska-Slabeva Katarina, Wozniak Thomas and Santi R (eds), *Grid and Cloud Computing: A Business Perspective on Technology and Applications* (Springer 2010).

Sztompka P, *Trust: A Sociological Theory* (Cambridge University Press 1999)

Taddeo M and Floridi L, ‘The Debate on the Moral Responsibilities of Online Service Providers’ in Taddeo M and Floridi L (eds), *Science and Engineering Ethics*, vol 22 (Springer 2016).

Tyler TR and Kramer RM, ‘Whither Trust’ in Tyler TR and Kramer RM (eds), *Trust in Organisations: Frontiers of Theory and Research* (Sage Publications 1996).

Uslaner EM, *The Moral Foundations of Trust* (CUP 2002).

Villegas D and others, ‘The Role of Grid Computing Technologies in Cloud Computing’ in Furht B and Escalante A (eds), *Handbook of Cloud Computing* (Springer 2010).

Voorsluys W, Broberg J and Buyya R, ‘Introduction to Cloud Computing’ in Rajkumar Buyya, James Broberg and Goscinski A (eds), *Cloud Computing: Principle and Paradigms* (John Wiley & Sons 2011).

Vu QH, Lupu M and Chin Ooi B, *Peer to Peer Computing : Principle and Application* (Springer 2010).

Walden I and Da Correggio Luciano L, ‘Facilitating Competition in the Clouds’ in Millard C (ed), *Cloud Computing* (OUP 2013).

Yee G, ‘Buidling Consumer Trust for Internet E-Commerce’ in Song R, Korba L and Yee G (eds), *Trust in E-Services: Technologies, Practices and Challenges: Technologies, Practices and Challenges* (Idea Group 2007).

Zanfir G, ‘Forgetting About Consent. Why the Focus Should be on “Suitable Safeguards” in Data Protection Law’ in Gutwirth S, Leenes R and De Hart P (eds), *Reloading the Data: Multidisciplinary Insights and Contemporary Challenges* (Springer 2013).

Journals

Abbadi IM and Alawneh M, ‘A Framework for Establishing Trust in the Cloud ’ (2012) 38 Computers and Electrical Engineering 1073.

Abbasi P, Bigham BS and Sarencheh S, ‘Good's History and Trust in Electronic Commerce’ (2011) 3 Procedia Comput Sci 827.

Abrams and M Crompton, ‘Multi–Layered Privacy Notices: A Better Way’ (2005) 2 Priv LB 1.

Aiken KD and Boush DM, ‘Trustmarks, Objective-Source Ratings, and Implied Investments in Advertising: Investigating Online Trust and the Context-Specific Nature of Internet Signals’ (2006) 34 JAMS 308.

Akerlof GA, ‘The Market for "Lemons": Quality Uncertainty and the Market Mechanism’ (1970) 84 Q J Econ 488.

Ambrose P and Chiravuri A, ‘An Empirical Investigation of Cloud Computing for Personal Use’ (2010) 24 MWAIS 2010 Proceedings 1.

Apostu A and others, ‘Study on Advantages and Disadvantages of Cloud Computing - The Advantages of Telemetry Applications in the Cloud’ (2013) Applied Computer Science 113.

Arutyunov VV, ‘Cloud Computing: Its History of Development, Modern State and Future Considerations’ (2012) 39 STIP 173.

Avizienis A and others, ‘Basic Concepts and Taxonomy of Dependable and Secure Computing’ (2004) 1 IEEE Transactions on Dependable and Secure Computing 11.

Bajpai S and Srivastava P, ‘A Fully Homomorphic Encryption Implementation on Cloud Computing’ (2014) 4 IJICT 811.

Balboni P, ‘Liability of Certification Service Providers Towards Relying Parties and the Need for a Clear System to Enhance the Level of Trust in Electronic Communication’ (2004) 13 ICT Law 211.

Balboni P, ‘Model for an Adequate Liability System for Trustmark Organisations’ (2006) 1 Privacy and Security Issues in Information Technology 97.

Balboni P and Pelino E, ‘Law Enforcement Agencies's Activities in the Cloud Environment: a European Legal Perspective’ (2013) 22 ICT Law 165.

Balboni P, Pelino E and Scudiero L, ‘Rethinking the One-Stop-Shop Mechanism: Legal Certainty and Legitimate Expectation’ (2014) 30 CLSR Rev 392.

Berry R and Reisman M, ‘Policy Challenge of Cross-Border Cloud Computing’ (2012) JICE 1.

Beugelsdijk S, Groot HLFd and Schaik ABTMv, 'Trust and Economic Growth: A Robustness Analysis' (2004) 56 Exford Economic Paper 118.

Boehm F, 'Data Processing and Law Enforcement Access to Information Systems at EU Level: No Consistent Framework in Spite of the Envisaged Data Protection Reform' (2012) 36 DuD 339.

Borghi M, Ferretti F and Karapapa S, 'Online Data Processing Consent Under EU Law: a Theoretical Framework and Empirical Evidence from the UK' (2013) 21 IJLIT 109.

Bradach JL and Eccles RG, 'Price, Authority and Trust : From Ideal Types to Plural Forms' (1989) 15 Annu Rev Sociol 97.

Brown I and Korff D, 'Foreign Surveillance: Law and Practice in a Global Digital Environment' 3 EHRLR 243.

Burney A, Asif M and Abbas Z, 'Forensics Issues in Cloud Computing' (2016) 4 JCC 63.

Buskens V, 'The Social Structure of Trust' (1988) 20 Soc Networks 265.

Buyya R and others, 'Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility' (2009) 25 FGCS 599.

Bygrave L, 'Determining Applicable Law Pursuant to European Data Protection Legislation' (2000) 16 CLSR 252.

Caldwell C and Karri R, 'Organizational Governance and Ethical Systems: A Covenantal Approach to Building Trust' (2005) 58 J Bus Ethics 249.

Calloway TJ, ‘Cloud Computing, Clickwrap Agreements, and Limitation on Liability Clauses : A Perfect Storm?’ (2012) 11 Duke L & Tech Rev 163.

Carolan E, ‘The Continuing Problems with Online Consent under the EU’Emerging Data Protection Principles’ (2016) 32 CLS Rev 462.

Chiregi Matin and Nima Jafari Navimipour, ‘A Comprehensive Study of the Trust Evaluation Mechanisms in the Cloud Computing’ (2017) 9 JoSS 1.

Ciocchetti CA, ‘The Future of Privacy Policies: A Privacy Nutrition Label Filled with Fair Information Practice ’ (2009) 26 J Marshall J Info Tech & Privacy L 1.

Corporate Illegality: Testing the Assumptions of the Corporate Sentencing Guidelines’ (2002) 37 J Bus Ethics 367.

Couillard DA, ‘Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing’ (2009) 93 Minn L Rev 2205.

Danidou Y and Schafer B, ‘Legal Environments for Digital Trust: Trustmarks, Trusted Computing and the Issue of Legal Liability’ (2012) 7 JICLT 212.

De Bruin B and Floridi L, ‘The Ethics of Cloud Computing’ (2017) 23 Sci Eng Ethics 32.

De Hert P and Papakonstantinou V, ‘The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System fo the Protection of Individuals’ (2012) 28 CLS Rev 130.

Deutsch M, ‘Trust, Trustworthiness and the F Scale’ (1960) 6(1) J Abnorm and Soc Psych 138.

Endeshaw A, ‘The Legal Significance of Trustmarks’ (2001) 10 ICT Law 203.

Esayas SY, ‘A Walk in to The Cloud and Cloudy It Remains: The Challenges and Prospects of 'Processing' and 'Transferring' Personal Data ’ (2012) 28 CLS Rev 662.

Ewing M, ‘The Perfect Storm: The Safe Harbour and the Directive on Data Protection’ (2002) 24 Hous J Int'l L 315.

Fernandes DAB and others, ‘Security Issues in Cloud Environments: A Survey’ (2013) 13 INT J INF SECUR 113.

Filippi PD and McCarthy S, ‘Cloud Computing: Centralization and Data Sovereignty’ (2012) 3 EJLT 1.

Francois P and Zabojnik J, ‘Trust, Social, Capital, and Economic Development’ (2005) 3 JEEA 51.

Gray A, ‘Conflict of Laws and the Cloud’ (2013) 29 CLS Rev 58.

Habib SM and others, ‘Trust as a Facilitator in Cloud Computing: A Survey’ (2012) 1 JoCCASA 1.

Hansen M, ‘Putting Privacy Pictograms Into Practice: A European Perspective’ (2009) 154 GI Jahrestagung 1703.

Harshbarger JA, ‘Cloud Computing Providers and Data Security Law: Building Trust with United States Companies’ (2011) 16 JTech L & Pol'y 229.

Hashizume K and others, ‘An Analysis of Security Issues for Cloud Computing’ (2013) 4 JISA 1.

Hayward R and Chiang C-C, ‘Parallelizing Fully Homomorphic Encryption for a Cloud Environment’ (2015) 13 J Appl Res Technol 245.

Hirschman AO, ‘Against Parimony : Three Easy Ways of Complicating Some Categories of Economic Discourse’ (1984) 74 Am Econ Rev 88.

Hon WK and others, ‘Policy, Legal and Regulatory Implications of a Europe-Only Cloud’ (2016) 24 IJLIT 251.

Huang J and Nicol DM, ‘Trust Mechanisms for Cloud Computing’ (2013) 2 JoCCASA 1.

Hurwitz JG, ‘Trust and Online Interaction’ (2013) 161 U Pa L Rev 1579.

Iram A and Khandekar A, ‘Homomorphic Encryption Method Applied to Cloud Computing’ (2014) 4 IJICT 1519.

Ismail UM and others, ‘A Framework for Security Transparency in Cloud Computing’ (2016) 8 Future Internet 1.

Jiang G, ‘Rain or Shine : Fair and Other Non-Infringing Uses in the Context of Cloud Computing’ (2010) 36 Journal of Legislation 395.

Jones K and Leonard LNK, ‘Trust in Consumer-to-Consumer Electronic Commerce’ (2008) 45 Inform Manage 88.

Katsh E, Rifkin J and Gaitenby A, ‘E-Commerce, E-Disputes, and E-Dispute Resolution: In the Shadow of “eBay Law’ (2000) 15 Ohio State Journal on Dispute Resolution 705.

Kesan PJ, Hayes CM and Bashir MN, ‘Information Privacy and Data Control in Cloud Computing ; Consumers, Privacy Preferences, and Market Efficiency’ (2013) 70 Wash & Lee L Rev 341.

Kim DJ, Ferrin DL and Rao HR, ‘A Trust-Based Consumer Decision-Making Model in Electronic Commerce: The Role of Trust, Perceived Risk and Their Antecedents’ (2008) 44 DSS 544.

King JN and Raja VT, ‘What Do They Really Know About Me in the Cloud? A Comparative Law Perspective on Protecting Privacy and Security of Sensitive Consumer Data’ (2013) 50 Am Bus LJ 413.

Koops B-J, ‘The Trouble with European Data Protection Law’ (2014) 4 IDPL 250.

Kouatlia I, ‘Managing Cloud Computing Environment: Gaining Customer Trust with Security and Ethical Management’ (2016) 91 Procedia Comput Sci 412.

Kovar SE, Burke KG and Kovar BR, ‘Consumer Responses to the CPA WEBTRUST™ Assurance’ (2000) 14 JIS 17.

Kraeuter SG, ‘The Role of Consumers' Trust in Online-Shopping’ (2002) 39 J Bus Ethics 43.

Lynn T and others, ‘Development of a Cloud Trust Label: A Delphi Approach’ (2016) 56 JCIS 185.

Macdonald E, ‘When is a Contract Formed by the Browse-Wrap Process?’ (2011) 19 IJLIT 285.

Matin C and Navimipour NJ, ‘A Comprehensive Study of the Trust Evaluation Mechanisms in the Cloud Computing’ (2017) 9 JoSS 1.

Mayer RC, Devis JH and Schoorman FD, ‘An Integrative Model of Organisational Trust’ (1995) 20 AMR 709.

McKnight DH and others, ‘Trust in Specific Technology: An Investigation of Its Components and Measures’ (2011) 2 ACM TMIS 12.

Moerel L, ‘The Long Arm of EU Data Protection Law: Does the Data Protection Directive Apply to Processing of Personal Data of EU Citizens by Websites Worldwide?’ (2011) 1 IDPL 28.

Moorman C, Deshpandé R and Zaltman G, ‘Factors Affecting Trust in Market Research Relationships’ (1993) 57 JM 81.

Morgan RM and Hunt SD, ‘The Commitment-Trust Theory of Relationship Marketing’ (1994) 58 JM 20.

Nissenbaum H, ‘Securing Trust Online : Wisdom or Oxymoron?’ (2001) 81 BUL Rev 101.

Noll J, ‘European Community & E-Commerce: Fostering Consumer Confidence’ (2002) 9 EDI L Rev 207.

Pateraki A, ‘EU Regulation Binding Corporate Rules Under the GDPR—What Will Change?’ (2016) 13 Bloomberg BNA World Data Protection Report 1.

Poteya MM, Dhoteb CA and Sharmac DH, ‘Homomorphic Encryption for Security of Cloud Data’ (2016) 79 Procedia Comput Sci 175.

Powell WW, ‘Neither Market Nor Hierarchy: Network Forms of Organization’ (1990) 12 Res Organ Behav 295.

Prince JD, ‘Introduction to Cloud Computing ’ (2011) 8 JERML 449.

Rashbaum KN, Borden BB and Beaumont TH, ‘Outrun the Lions: A Practical Framework for Analysis of Legal Issues in the Evolution of Cloud Computing’ (2014) 12 Ave Maria L REV 71.

Ratnasingam P, ‘Trust in Inter-Organizational Exchanges: a Case Study in Business to Business Electronic Commerce’ (2005) 39 Decis Support Syst 525.

Richard N and Hartzog W, ‘Taking Trust Seriously in Privacy Law’ (2015) 19 Standford Technology Law Review 431.

Rifon NJ, Larose R and Choi SM, ‘Your Privacy Is Sealed: Effects of Web Privacy: Seals on Trust and Personal Disclosures’ (2005) 39 JCA 339.

Robinson WJ, ‘Free at What Cost? Cloud Computing Privacy Under the Stored Communications Act ’ (2010) 98 Geo L J 1195.

Rohrmann CA and Rocha Cunha JFS, ‘Some Legal Aspects of Cloud Computing Contracts’ (2015) 10 JICLT 37.

Rotter JB, ‘Interpersonal Trust, Trustworthiness, and Gullibility.’ (1980) 35 Am Psychol 1.

Rousseau DM and others, ‘Not so Different After All : a Cross-Discipline View of Trust’ (1998) 23 AMR 393.

Schwartz PM, ‘EU Privacy and the Cloud: Consent and Jurisdiction Under the Proposed Regulation’ (2013) 12 PVLR 718.

——, ‘Information Privacy in the Cloud ’ (2013) 161 U Pa L Rev 1623.

Seligman AB, ‘Trust and Sociability: On the Limits of Confidence and Role Expectations’ (1988) 57 AJES 391.

Sergent RS, ‘Cloud Computing and Ethics’ (2011) 44 MSBA 24.

Simou S and others, ‘A Survey on Cloud Forensics Challenges and Solutions’ (2016) 9 Security and Communication Networks 6285.

Solove DJ, ‘Introduction: Privacy Self-Managemen and the Consent Dilemma’ (2013) 126 Harv L Rev 1880.

Sun D and others, ‘Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environments’ (2011) 15 PE 2852.

Svantesson DJB, ‘Article 4(1)(a) ‘Establishment of the Controller” in EU Data Privacy Law – Time to Rein in This Expanding Concept?’ (2016) 6 IDPL 210.

Svantesson D and Clarke R, ‘Privacy and Consumer Risks in Cloud Computing’ (2010) 26 CLS Rev 391.

Svensson G and Wood G, ‘A Model of Business Ethics’ (2008) 77 J Bus Ethics 303.

Swire P and Kennedy-Mayo D, ‘How Both the EU and the US are “Stricter” Than Each Other for the Privacy of Government Requests for Information ’ (2017) 66 Emory Law Journal 671.

Taddeo M and Floridi L, 'The Debate on the Moral Responsibilities of Online Service Providers' (2016) 22 Sci Eng Ethics 1575.

Tang F-F and others, *Using Insurance to Create Trust on the Internet* (2003) 46 Communication of the ACM 337.

Taylor M and others, 'Forensic Investigation of Cloud Computing Systems' (2011) 3 Network Security 4.

TEBAA M and HAJII SE, 'Secure Cloud Computing through Homomorphic Encryption' (2013) 5 IJACT 2013.

Terry NP, 'Rating the Raters: Legal Exposure of Trustmark Authorities in the Context of Consumer Health Informatics' (2000) 2 JMIR 1.

Trope RL and Hughes SJ, 'Red Skies in the Morning - Professional Ethics at the Dawn of Cloud Computing' (2011) 38(1) Wm Mitchell L Rev 111.

Turculet M, 'Ethical Issues Concerning Online Social Networks' (2014) 149 Procedia Soc Behav Sci 967.

Van Den Ber B and Van Der Hof S, 'What Happens to my Data? A Novel Approach to Informing Users of Data Processing Practices' (2012) 7 First Monday 1.

Voss WG, 'Looking at European Union Data Protection Law Reform through a Different Prism: the Proposed EU General Data Protection Regulation Two Years Later' (2014) 17 J Internet L 11.

Watts S, 'Corporate Social Responsibility Reporting Platforms: Enabling Transparency for Accountability' (March 2015) 16 Information Technology and Management 19.

Webber M, ‘The GDPR’s Impact on the Cloud Service Provider as a Processor’ (2016) 16 PDP J 11.

Wendel PT, ‘The Evolution of the Law of Trustee’s Powers and Third Party Liability for Participating in a Breach of Trust: An Economic Analysis’ (2005) 35 Seton Hall L Rev 971.

Whitehouse D and others, ‘Twenty-five Years of ICT and Society: Codes of Ethics and Cloud Computing’ (2015) 45 SIGCAS Computers & Society 18.

WJ A, B B and A B, ‘Specific Inactivation of the Phospohydrolase Component of the Hepatic-Microsomal Glucose-6-Phosphatase System by Diethyl Pyrocarbonate’ (1984) 220 Biochem J 835.

Yunchuan S and others, ‘Data Security and Privacy in Cloud Computing’ (2014) IJDSN 1.

Zack PJ and Knach S, ‘Trust and Growth’ (2001) 111 EJ 295.

Zhou L, Varadharajan V and Hitchens M, ‘Secure Administration of Cryptographic Role-Based Access Control for Large-Scale Cloud Storage Systems’ (2014) 80 JCSS 1518.

Others

A29WP, *Explanatory Document on the Processor Binding Corporate Rules* (00658/13/EN WP 204 rev01, Adopted on 19 April 2013 As last revised and adopted on 22 May 2015).

——, *Opinion 4/2007 on The Concept of Personal Data* (01248/07/EN WP 136, Adopted 20 June 2007).

——, *Opinion 1/2008 on Data Protection Issues Related to Search Engines* (00737/EN WP 148, Adopted on 4 April 2008).

——, *Opinion 1/2010 on The Concepts of "Controller" and "Processor"* (00264/10/EN WP 169, Adopted 16 February 2010).

——, *Opinion 8/2010 on Applicable Law* (0836-02/10/EN WP 179, Adopted 16 December 2010).

——, *Opinion 15/2011 on the Definition of Consent* (01197/11/EN WP187, Adopted 13 July 2011).

——, *Opinion 1/2012 on the Data Protection Reform Proposals* (00530/12/EN WP 191, Adopted 23 March 2012).

___, *Opinion 5/2012 on Cloud Computing* (01037/12/EN WP196, Adopted 1 July 2012).

___, *Opinion 4/2014 on Surveillance of Electronic Communications for Intelligence and National Security Purposes* (819/14/EN WP 215, Adopted on 10 April 2014).

——, *Opinion 8/2014 on the on Recent Developments on the Internet of Things* (14/EN WP 223, Adopted on 16 September 2014).

——, *Opinion 1/2016 on the EU – U.S. Privacy Shield Draft Adequacy Decision* (16/EN WP 238, Adopted on 13 April 2016).

—, *Working Document on a Common Interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995* (2093/05/EN WP 114, Adopted 25 November 2005).

—, *Working Document on Surveillance of Electronic Communications for Intelligence and National Security Purposes* (14/EN WP 228, Adopted 5 December 2014).

Aleecia M MacDonald, Robert W Reeder, Patrick Gage Kelley, L F Cranor, "*A Comparative Study of Online Privacy Policies and Formats"* (2009) in Privacy Enhancing Technologies, 5672 Lecture Notes in Computer Science.

Alleweldt F and others, *Cloud Computing* (European Parliament's Committee on Internal Market and Consumer Protection, 2012).

Alleweldt F and others, *A Pan European Trustmark for E-Commerce: Possibilities and Opportunities* (Policy Department A: Economic and Scientific Policy, July 2012).

Armbrust M and others, *Above the Clouds : A Berkeley View of Cloud Computing* (Technical Report No UCB/EECS-2009-28 (10 February 2009)).

Balboni P, *Third-Party Liability of Trustmark Organisations in Europe* (Tilburgh University Publication, 2008).

Bigo D and others, *Fighting Cyber Crime and Protecting Privacy in the Cloud* (The European Parliament's Committee on Civil Liberties, Justice and Home Affairs 2012).

Buest R and Miller P, *The State of Europe's Homegrown Cloud Market* (GIGAOM Research, A Cloud Report, 17 Sept 2013).

Commission, *Communication from the Commission to the European Parliament and the Council: Exchanging and Protecting Personal Data in a Globalised World* (Brussels, 1012017, COM(2017) 7 final).

——, *Comparative Study on Cloud Computing Contracts* (Prepared by DLA Piper UK LLP March 2015).

___, *EU Online Trustmarks Building Digital Confidence in Europe: Final Report* (2012).

——, *Report from the Commission- First Report on the Implementation of the Data Protection Directive (95/46/EC)* (Brussels, 1552003 COM(2003) 265 final).

——, *Special Eurobarometer 431 on Data Protection* (March 2015).

——, *Towards a Thriving Data-Driven Economy* (Brussels, 272014 COM(2014) 442 final).

——, *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*, (Brussels, 20102004 SEC (2004) 1323).

——, *Unleashing the Potential of Cloud Computing in Europe* (Brussels, 2792012 COM(2012) 529 final).

——, *Working Document on a Common Interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995* (Adopted on 25 November 2005, 2093/05/EN WP 114).

——, *Working Document on Determining the International Application of EU Data Protection Law to Personal Data Processing on the Internet by Non-EU Based Web Sites* (5035/01/EN/Final WP 56, Adopted on 30 May 2002).

——, *Working Document: Transfers of Personal Data to Third Countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers* (11639/02/EN WP 74, Adopted 3 June 2003).

——, *Working Document Setting up a Framework for the Structure of Binding Corporate Rules* (1271-00-01/08/EN WP 154, Adopted on 24 June 2008).

——, *Working Document Setting up a Table with the Elements and Principles to be Found in Binding Corporate Rules* (1271-00-00/08/EN WP 153, Adopted on 24 June 2008).

——, *Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules* (1271-04-02/08/EN WP 155 rev04, Adopted on 24 June 2008 as last Revised and adopted on 8 April 2009).

——, *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*(Brussels, 25.1.2012 COM (2012) 11 final).

——, *Legislation L119* (4 May 2016) 59 OJEU.

Damon A and others, *Developing Internet Consumer Trust: Exploring Trustmarks As Third-Party Signals* (AMA Winter Educators' Conference Proceedings, 2003).

De Bruin R and others, *Analysis and Definition of Common Characteristics of*

Trustmarks and Web Seals in the European Union (Final Report, February 2005).

EDPS, *Opinion 4/1026 on the EU-U.S. Privacy Shield Draft Adequacy Decision* (30 May 2016).

Edwards L and Theunissen A, *Creating Trust and Satisfaction Online: How Important Is ADR? The UK eBay Experience* (21st BILETA Conference: Globalisation and Harmonisation in Technology Law, Malta, April 2006).

Einwiller S, *The Significance of Reputation and Brand for Creating Trust in the Different Stages of a Relationship between an Online Vendor and its Customers* (Eighth Research Symposium on Emerging Electronic Markets, 2001).

ENISA, *An SME Perspective on Cloud Computing : Survey* (June 2010).

___, *Cloud Computing : Benefits, Risks And Recommendations for Information Security* (December 2012).

——, *Consumerization of IT: Top Risks and Opportunities : Responding to the Evolving Threat Environment* (2012).

___, On the Security, Privacy and Usability of Online Seals: An Overview (December 2013).

___, *Study on the Use of Cryptographic Techniques in Europe* (20 April 2012).

Faragardi HR, *Ethical Considerations in Cloud Computing Systems* (Summit Digitalisation for a Sustainable Society, Gothenburg, Sweden, 12–16 June 2017).

Fosci M and Johnson R, *Market Engagement in the Databox Project* (Summary Report Results of the Stakeholder Consultation Prepared on Behalf of Horizon Digital Economy Institute, October 2017).

Foster I and others, *Cloud Computing and Grid Computing 360-Degree Compared* (Grid Computing Environments Workshop (GCE) 12-16 November, 2008).

FTC, *Court Halts U.S. Internet Seller Deceptively Posing as U.K. Home Electronics Site* (FTC File No 092-3081, 6 August 2009).

G Kelley et al., *Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach* (2010) Carnegie Mellon University, CyLab, Technical Reports, CMU–CyLab.

Graf C and others, *Towards Usable Privacy Enhancing Technologies: Lessons Learned from the PrimeLife Project* (17 June 2011) 19.

Habib SM, Ries S and Muhlhauser M, *Towards a Trust Management System for Cloud Computing* (2011) International Joint Conference of IEEE TrustCom-11/IEEE ICESS-11/FCST-11 933.

Holtz L-E, Nocun K and Hansen M, *Towards Displaying Privacy Information with Icons* (352 IFIP Advances in Information and Communication Technology 338, 2011).

Hon WK and others, *Cloud Accountability: The Likely Impact of the Proposed EU Data Protection Regulation* (Tilburg Law School Legal Studies Research Paper Series, No 07/2014).

ICO, *Guideline on the Use of Cloud Computing* (9 May 2013).

—, *Proposed New EU General Data Protection Regulation: Article-by-Article Analysis Paper* (V10 12 February 2013).

Jansen W and Grance T, *Guidelines on Security and Privacy in Public Cloud Computing* (Report of the National Institute of Standards and Technology, January 2011).

Jayaram KR and others, *Trustworthy Geographically Fenced Hybrid Clouds* (In ACM/IFIP/USENIX 15th International Middleware Conference, Dec 2014).

Kanwal A and others, *Assessment Criteria for Trust Models in Cloud Computing* (2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing 2013).

Ko R, Lee B.S. and Pearson S, 'Towards Achieving Accountability, Auditability and Trust in Cloud Computing' in Abraham A and others (eds), *Advances in Computing and Communications* (first International Conference, ACC 2011, Kochi, India, July 22-24, 2011. Proceedings, Part I).

Kroes N, *EU Data Protection Reform and Cloud Computing* (Data Protection Reform and Cloud Computing "Fuelling the European Economy" Event, Brussels, 30 January 2012 SPEECH/12/40).

Kuner C, *The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law* (Bloomberg BNA Privacy and Security Law Report 6 February 2012)

Labelinsight, *Driving Long- Term Trust and Loyalty Through Transparency* (The 2016 Label Insight Transparency ROI Study).

Lauter K, Naehrig M and Vaikuntanathan V, *Can Homomorphic Encryption be*

Practical? (In Proceeding ACM Cloud Computing Security Workshop, 2011).

Leenes R, *Who Controls the Cloud?* (6th IDP Conference Cloud Computing: Law and Politics in The Cloud 2010).

Lynn T and others, *The Case for Cloud Service Trustmarks and Assurance-As-A-Service* (International Conference on Cloud Computing and Service Science CLOSER 2013).

McAuley D, Mortier R and Goulding J, *The Dataware Manifesto* (Proceedings of the 3rd International Conference on Communication Systems and Networks, Bangalore, IEEE, 2011).

Meissner S, *Privacy Seals: The European Privacy Seal EuroPriSe* (DataEthics: Building Digital Trust –Hellerup, 19 May 2016).

Meixner F and Buettner R, *Trust as an Integral Part for Success of Cloud Computing* (ICIW 2012 : The Seventh International Conference on Internet and Web Applications and Services 2012).

Mell P and Grance T, *The NIST Definition of Cloud Computing* (Recommendation of the National Institute of Standards and Technology, 2011).

Moreno EA and others, *Digital Memories: Ethical Perspective* (Summary Report on the Workshop Held at JRC, European Commission, Ispra, Italy, 16th - 17th January 2014).

Mortier R and others, *Personal Data Management with the Databox: What's Inside the Box?* (Proceedings of the 2016 ACM Workshop on Cloud-Assisted Networking: December 12, 2016, Irvine, CA, USA).

Nordquist F, Andersson F and Dzepina EN, *Trusting the Trustmark?* (17th BILETA Annual Conference April 5th - 6th, 2002, Free University, Amsterdam).

Papanikolaou N, Pearson S and Wainwrigh N, *Accountability in Cloud Computing* (Building International Cooperation for Trustworthy Discussion Paper, 22 June 2011).

Parliament E, *Commission Implementing Decision of 12.7.2016 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield* (Brussels, 1272016 C(2016) 4176 final).

Pearson S and Benameur A, *Privacy, Security and Trust Issues Arising from Cloud Computing* (The 2nd International Conference on Cloud Computing 2010, Indiana, USA 2010).

Pearson S and others, *Accountability for Cloud and Other Future Internet Services* (IEEE 4th International Conference on Cloud Computing Technology and Science, 2012).

Povey D, *Developing Electronic Trust Policies Using a Risk Management Model* (Proceedings of 1999 CQRE (Secure) Congress, Germany, 1999).

Rauhofer J and Bowden C, *Protecting Their Own:Fundamental Rights Implications for EU Data Sovereignty in the Cloud* (Edinburgh School of Law Research Paper Series No 2013/28).

Rundle M, *International Personal Data Protections and Digital Identity Management Tools* (Position Paper Submitted for the W3C Workshop on Languages for Privacy Policy Negotiation and Semantics-Driven Enforcement, Italy, 13 September 2006).

Sen J, 'Security and Privacy Issues in Cloud Computing' in Martinez R, Garcia P and Lopez M (eds), *Architectures and Protocols for Secure Information Technology; Information Science Reference: Hershey, PA, USA* (IGI Global 2013).

Singh J and others, *Regional Clouds: Technical Considerations* (Technical Report Number 863, November 2014).

Srinivasan S, *Building Trust in Cloud Computing: Challenges in the Midst of Outrages* (2014) Proceedings of Information Science & IT Education Conference 305.

Timmermans J and Ikonen V, *The Ethics of Cloud Computing: A Conceptual Review* (Cloud Computing, Second International Conference, CloudCom 2010, November 30 - December 3, 2010, Indianapolis, Indiana, USA).

Titulescu N, 'Cloud Computing Services: Benefits, Risks and Intellectual Property Issues' (2014) 2(1) University of Bucharest, Faculty of Economic Sciences;Institute for World Economy of the Romanian Academy 230.

Wanne Pemmelaar, Van Der Leeuw-Veiksha A and Mullarkey C, *BCRs under the GDPR: Practical Considerations* (PL&B UK Reports, March 2017).

Werff LVD and others, 'Building Trust in the Cloud Environment: Towards a Consumer Cloud Trust Label' (2014) ICDS 2014: The Eighth International Conference on Digital Society.

WPPJ AWa, 'The Future of Privacy : Joint Contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data' 02356/09/EN, WP 168 Adopted on 01 December 2009.

Websites

Abboud L and Paul S, ‘Analysis - European Cloud Computing Firms See Silver Lining in Prism Scandal’ 17 June 2013 <http://uk.reuters.com/article/uk-cloud-europe-spying-idUKBRE95G0FM20130617> accessed 11 July 2017.

Accenture, ‘Digital Trust in IoT Era’ 2015 <https://www.accenture.com/t20160318T035041__w__/us-en/_acnmedia/Accenture/Conversion-Assets/LandingPage/Documents/3/Accenture-3-LT-3-Digital-Trust-IoT-Era.pdf> accessed 1 May 2017.

Administration TUT, ‘European Union - Labeling/Marking Requirements’ (*19 July 2017*) <https://www.export.gov/article?id=European-Union-Marking-Labeling-and-Packaging-Overview> accessed 1 January 2018.

Alliance CS, ‘Top Threats to Cloud Computing Report (Ver.1.0)’ 2010 <https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf> accessed 1 March 2015

——, ‘Top Threats to Cloud Computing: Survey Results Update 2012’ <https://downloads.cloudsecurityalliance.org/initiatives/top_threats/Top_Threats_Cloud_Computing_Survey_2012.pdf> accessed 11 July 2017

‘Amazon's Useless "Transparency Reports" Won't Disclose Whether They're Handing Data From Always-on Alexa Mics to Governments’ (*18 January 2018*) <https://boingboing.net/2018/01/18/nunya-bizness.html> accessed 1 February 2018.

Amazon, ‘Transparency Report’ <http://d0.awsstatic.com/certifications/Information_Request_Report.pdf> accessed 1 January 2018.

Authur C, ‘Fears Over NSA Surveillance Revelations Endanger US Cloud Computing Industry’ The Guardian, 8 August 2013

<http://www.theguardian.com/world/2013/aug/08/nsa-revelations-fears-cloud-computing> accessed 1 July 2017.

Cardozo N and others, 'Who Has Your Back? 2017: The Electronic Frontier Foundation's Seventh Annual Report on Online Service Providers' Privacy and Transparency Practices Regarding Government Access to User Data' (*July 2017*) <https://www.eff.org/files/2017/07/08/whohasyourback_2017.pdf> accessed 11 January 2018.

Centre DC, 'Trust in Personal Data : A UK Review' 2014 <http://www.digitalcatapultcentre.org.uk/wp-content/uploads/2015/07/Trust-in-Personal-Data-A-UK-Review.pdf> accessed 1 January 2016.

Cloud C, 'Overview Report of Legal and Regulatory Requirements in Data Management' (*Coco Cloud: Confidential and Compliant Clouds, D2.1, 30 April 2014*) <http://www.coco-cloud.eu/sites/default/files/cococloud/files/content-files/deliverables/Coco_Deliverable D2.1_UO_20140430.pdf> accessed 1 January 2016.

Cloud G, 'EU Data Protection Authorities Confirm Compliance of Google Cloud Commitments for International Data Flows' (2 February 2017) <https://blog.google/topics/google-cloud/eu-data-protection-authorities-confirm-compliance-google-cloud-commitments-international-data-flows/> accessed 1 March 2017.

Commission, 'Data Protection Eurobarometer: Fact Sheet' June 2015 <http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_eurobarometer_240615_en.pdf> accessed 1 May 2017.

Connolly C, 'Trustmark Schemes Struggle to Protect Privacy' (*26 September 2008*)

<http://www.galexia.com/public/research/assets/trustmarks_struggle_20080926/> accessed 12 January 2018.

Consulting F, 'Personal Cloud Services Emerge To Orchestrate Our Mobile Computing Lives' July 2012 <https://www.sugarsync.com/media/sugarsync-forrester-report.pdf> accessed 1July 2017.

Cowen T, 'Competition Law Issues in Cloud Computing' (2013) <http://www.scl.org/site.aspx?i=ed30526> accessed 1 March 2014.

CyLab Centre at Carnegie Mellon University, 'Privacy Nutrition Labels' (*6 March 2013*) <http://www.openlawlab.com/2013/06/03/privacy-nutrition-labels/> accessed 1 January 2018.

Dell, 'Cloud Computing : A Dell Point of View' <https://communities.vmware.com/.../Nicolai Sandager - Dell.p..> accessed 16 July 2017.

Dropbox, 'Transparency Overview' < https://www.dropbox.com/transparency> and 'Transparency Report'<https://www.dropbox.com/transparency/reports>accessed 1 January 2018.

EY, 'Corporate Misconduct — Individual Consequences Global Enforcement Focuses the Spotlight on Executive Integrity 14th Global Fraud Survey' 2016 <http://www.ey.com/Publication/vwLUAssets/ey-global-fraud-survey-2016/$FILE/ey-global-fraud-survey-final.pdf> accessed 1 May 2017.

Forrest E, 'Privicons Released: A User-to-User Email Privacy Tool' (*21 November 2011*) <http://cyberlaw.stanford.edu/blog/2011/11/privicons-released-user-user-email-privacy-tool> accessed 1 January 2018.

Forrest E and Schallaböck J, 'Privicons: An Approach to Communicating Privacy Preferences Between Users' Stanford/Berlin November, 2010 <https://www.iab.org/wp-content/IAB-uploads/2011/03/jan_schallabock.pdf> accessed 1 January 2010.

Forum CI, 'Lack of Trust Holding Back Further Cloud Adoptions, Finds Cloud Industry Forum' June 2015 <https://www.cloudindustryforum.org/content/lack-trust-holding-back-further-cloud-adoptions-finds-cloud-industry-forum> accessed 20 December 2015.

Foundation TITI, 'How Much Will PRISM Cost the U.S. Cloud Computing Industry?' August 2013 <http://www2.itif.org/2013-cloud-computing-costs.pdf> accessed 1 June 2017.

Fulbright NR, 'Global Data Privacy Directory' (*July 2014*) <http://www.nortonrosefulbright.com/files/global-data-privacy-directory-52687.pdf> accessed 1 March 2017.

Funambol, 'Personal Cloud Survey: Hype vs. Reality' Research Report, August 2011 <http://www.funambol.com/documents/Funambol_PersonalCloudSurvey_Aug11.pdf> accessed 20 July 2017.

Google, 'Google Transparency Report' <https://transparencyreport.google.com> accessed 1 January 2018.

Google, 'Government Requests to Remove Content' <https://transparencyreport.google.com/government-removals/overview> accessed 1 January 2018.

Google, 'Requests for User Information' <https://transparencyreport.google.com/user-data/overview> accessed 1 January 2018.

Google, 'Traffic and Disruptions' <https://transparencyreport.google.com/traffic/overview> accessed 1 January 2018.

Hon WK, 'Killing Cloud Quickly, with GDPR' (4 Febuary 2016) <http://www.scl.org/site.aspx?i=ed46375> accessed 1 November 2016.

Horrigan JB, 'Use of Cloud Computing Applications and Services' Pew Research Center, September 2008 <http://www.pewinternet.org/2008/09/12/use-of-cloud-computing-applications-and-services/> accessed 1 May 2017.

House TW, 'Executive Order: Enhancing Public Safety in the Interior of the United States' (*25 January 2017*) <https://www.whitehouse.gov/the-press-office/2017/01/25/presidential-executive-order-enhancing-public-safety-interior-united> accessed 1 March 2017.

HP Corporate Ethics <http://www8.hp.com/us/en/hp-information/global-citizenship/governance/ethics.html> accessed 1 March 2018.

IBM, 'IBM Opens First Cloud Data Center With SoftLayer in Germany' 7 January 2015 <http://www-03.ibm.com/press/us/en/pressrelease/45786.wss> accessed 11 July 2017.

IDC, 'Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Up-take' SMART 2011/0045, 13 July 2012 <http://cordis.europa.eu/fp7/ict/ssai/docs/study45-d2-interim-report.pdf> accessed 1 May 2017.

Institute FR, 'Personal Data in the Cloud: A Global Survey of Consumer Attitudes' Technical Report, 2010 <http://www.fujitsu.com/downloads/SOL/fai/reports/fujitsu_personal-data-in-the-cloud.pdf> accessed 1 July 2017.

Peters RG, Covello VT and McCallum DB, 'The Determinants of Trust and Credibility in Environmental Risk Communication: An Empirical Study' Risk Analysis, 17(1) 43-54<http://centerforriskcommunication.org/publications/Environmental_Risk_Trust_Credibility_Factors_Study.pdf> accessed 1 July 2017.

Plummer DC and others, 'Cloud Computing : Defining and Describing an Emerging Phenomenon' Gartner,17 June 2008 <http://www.emory.edu/BUSINESS/readings/CloudComputing/Gartner_cloud_computing_defining.pdf> accessed 1 June 2017.

PrimeLife WP4.3. UI Prototypes: Policy Administration and Presentation – Version 2. In S. Fischer-H¨ubner and H. Zwingelberg, editors, PrimeLife Deliverable D4.3.2. PrimeLife, http://www.{PrimeLife}.eu/results/documents, June 2010.

Privacy and Identity Management in Europe for Life' (2008) <http://primelife.ercim.eu/results/documents/> accessed 1 January 2018.

Raskin A, 'Privacy Icons: Alpha Release' <http://www.azarask.in/blog/post/privacy-icons/> accessed 1 January 2018.

Reding V, 'PRISM Scandal: Vice-President Reding Makes it Clear the Data Protection Rights of EU Citizens are Non-Negotiable' (*EU-U.S. Ministerial held on 14 June 2013.*, 2013)<http://ec.europa.eu/commission_2010-2014/reding/multimedia/news/2013/06/20130612_en.htm> accessed 11 May 2014.

Salgado R and Chavez P, 'A Petition for Greater Transparency' (*9 September 2013*) <https://www.blog.google/topics/public-policy/petition-greater-transparency/> accessed 1 January 2018.

Salow H, 'Keeping your Intellectual Property in the Cloud' Intellectual Asset Management March/April 2014 <https://thomsonipmanagement.com/docs/downloads/iam_cloud_software_hsalow_0214.pdf> accessed 1 November 2014.

Schmidt S, 'Privacy and Data Security' (*12 June 2015*) <https://aws.amazon.com/blogs/security/privacy-and-data-security/> accessed 11 January 2018.

Statista, 'Number of Daily Active Facebook Users Worldwide 2011-2015' <http://www.statista.com/statistics/346167/facebook-global-dau/> accessed 9 July 2017.

Strickland J, 'How Cloud Computing Works ' (2008) <http://computer.howstuffworks.com/cloud-computing/cloud-computing1.htm> accessed 11July 2017.

Taylor S and Bornocp L, 'Cloud Computing: Competition Law Challenges' (2011) <http://www.scl.org/site.aspx?i=ed22705> accessed 1 March 2014.

Transparency Reporting Index (2016) <https://www.accessnow.org/tri> accessed 1 January 2018.

TRUSTe & Disconnect Introduce Visual Icons to Help Consumers Understand Privacy Policies' (*23 June 2014*) <http://www.trustarc.com/blog/2014/06/23/truste-disconnect-introduce-visual-icons-to-help-consumers-understand-privacy-policies/> accessed 1 January 2018.

Urquhart J, 'FBI Seizures Highlight Law as Cloud Impediment' (*CNET, 22 April 2009*) <http://www.cnet.com/uk/news/fbi-seizures-highlight-law-as-cloud-impediment/> accessed 11 March 2014.

US Department of Commerce, 'European Union - Labeling/Marking Requirements' (*19 July 2017*) <https://www.export.gov/article?id=European-Union-Marking-Labeling-and-Packaging-Overview> accessed 1 January 2018.

US Tech Giants Are Investing Billions to Keep Data in Europe, 3 Oct 2016 <https://www.nytimes.com/2016/10/04/technology/us-europe-cloud-computing-amazon-microsoft-google.html> access 1 March 2018.

Venkatraman A, 'Cloud Providers Rush to Build European Data Centres over Data Sovereignty' (*14 October 2014*) <http://www.computerweekly.com/news/2240233331/Cloud-providers-rush-to-build-European-datacentres-over-data-sovereignty> accessed 1 January 2017.

Whittaker Z, 'Amazon Doesn't Want You to Know How Many Data Demands It Gets' (*19 March 2015*) <http://www.zdnet.com/article/amazon-dot-com-the-tech-master-of-secrecy/> accessed 11 February 2018.

Yahoo, 'Yahoo is Now Part of Oat'. <https://policies.yahoo.com/ie/en/yahoo/privacy/euoathnoticefaq/> accessed 11 January 2018.

Yoti YUKa, 'British Opinions on Identity and Personal Information' 2017 <https://get.yoti.com/yougov-results/yougov-report-2/> accessed 1 May 2017.