Perspectives in Law, Business and Innovation

Marcelo Corrales
Mark Fenwick
Nikolaus Forgó *Editors*

New Technology, Big Data and the Law

KYUSHU
UNIVERSITY

Springer

Perspectives in Law, Business and Innovation

Over the last three decades, interconnected processes of globalization and rapid technological change—particularly, the emergence of networked technologies—have profoundly disrupted traditional models of business organization. This economic transformation has created multiple new opportunities for the emergence of alternate business forms, and disruptive innovation has become one of the major driving forces in the contemporary economy. Moreover, in the context of globalization, the innovation space increasingly takes on a global character. The main stakeholders—innovators, entrepreneurs and investors—now have an unprecedented degree of mobility in pursuing economic opportunities wherever they arise. As such, frictionless movement of goods, workers, services, and capital is becoming the "new normal".

This new economic and social reality has created multiple regulatory challenges for policymakers as they struggle to come to terms with the rapid pace of these social and economic changes. Moreover, these challenges impact across multiple fields of both public and private law. Nevertheless, existing approaches within legal science often struggle to deal with innovation and its effects.

Paralleling this shift in the economy, we can, therefore, see a similar process of disruption occurring within contemporary academia, as traditional approaches and disciplinary boundaries—both within and between disciplines—are being re-configured. Conventional notions of legal science are becoming increasingly obsolete or, at least, there is a need to develop alternative perspectives on the various regulatory challenges that are currently being created by the new innovation-driven global economy.

The aim of this series is to provide a forum for the publication of cutting-edge research in the fields of innovation and the law from a Japanese and Asian perspective. The series will cut across the traditional sub-disciplines of legal studies but will be tied together by a focus on contemporary developments in an innovation-driven economy and will deepen our understanding of the various regulatory responses to these economic and social changes.

More information about this series at http://www.springer.com/series/15440

Marcelo Corrales · Mark Fenwick
Nikolaus Forgó
Editors

New Technology, Big Data and the Law

Springer

Editors
Marcelo Corrales
Institute for Legal Informatics
Leibniz Universität Hannover
Hannover
Germany

Nikolaus Forgó
Institute for Legal Informatics
Leibniz Universität Hannover
Hannover
Germany

Mark Fenwick
Faculty of Law
Kyushu University
Fukuoka
Japan

ISSN 2520-1875 ISSN 2520-1883 (electronic)
Perspectives in Law, Business and Innovation
ISBN 978-981-10-5037-4 ISBN 978-981-10-5038-1 (eBook)
DOI 10.1007/978-981-10-5038-1

Library of Congress Control Number: 2017944287

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

Preface

This volume is part of the book series: *Perspectives in Law, Business and Innovation*. The aim of this series is to provide a forum for the publication of cutting-edge research in the fields of innovation and the law from a Japanese and Asian perspective. The series aims to cut across the traditional sub-disciplines of legal studies, but will be tied together by a focus on deepening our understanding of the various regulatory responses to these technological, economic and social changes.

This volume constitutes the result of a joint cooperative effort drawing on the extensive global network of two academic institutions: The Institute for Legal Informatics (IRI), part of the Law Faculty of the Leibniz Universität Hannover (Hannover, Germany), and the Graduate School of Law, Kyushu University (Fukuoka, Japan). Contributors to this book—including legal and software engineering scholars and practitioners from Europe, East Asia and the Americas—attempt to provide some of the latest thinking and assessment of current regulations with regard to emerging web-based technologies, Internet applications and related systems.

The main target audiences of the book are two different groups. The first group belongs to the legal community—particularly, legal scholars, law students and practitioners—in the field of IT and IP Law who are interested in an up to date legal analysis of current Internet trends. The second group are IT experts in the field of Cloud Computing, Big Data and Internet of Things—including, service and infrastructure providers, IT managers, Chief Executive Officers (CEOs), Chief Information Officers (CIOs) and software developers—who are interested and influenced by some of the shortcomings and benefits of the current legal issues under scrutiny in this work.

The editors would like to thank the Editor-in-Chief of this book series, Prof. Toshiyuki Kono, for opening the doors to this book project and for his constant support. The editors are also indebted to the authors and co-authors of each chapter for their hard work, patience and cooperation throughout the whole process from initial concept to the final manuscript. Finally, the editors are grateful to the Springer staff for their support and efforts in ensuring final publication.

Hannover, Germany — Marcelo Corrales
Fukuoka, Japan — Mark Fenwick
Hannover, Germany — Nikolaus Forgó
March 2017

Contents

Contributors

Daniel Bunge Attorney, New York, NY, USA

Marcelo Corrales Institute for Legal Informatics, Leibniz Universität Hannover, Hannover, Germany

Karim Djemame School of Computing, University of Leeds, Leeds, UK

Mark Fenwick Graduate School of Law, Kyushu University, Fukuoka, Japan

Nikolaus Forgó Institute for Legal Informatics, Leibniz Universität Hannover, Hannover, Germany

Yuriko Haga Faculty of Law, Kanazawa University, Kanazawa, Japan

Christian Hawellek Institute for Legal Informatics, Leibniz Universität Hannover, Hannover, Germany

Stefanie Hänold Institute for Legal Informatics, Leibniz Universität Hannover, Hannover, Germany

Paulius Jurčys Popvue Inc., San Francisco, USA

Friederike Knoke Institute for Legal Informatics, Leibniz Universität Hannover, Hannover, Germany

George Kousiouris Department of Electrical and Computer Engineering, National Technical University of Athens, Athens, Greece

Cecilia Magnusson Sjöberg Faculty of Law, Stockholm University, Stockholm, Sweden

Ugo Pagallo Giurisprudenza, Università di Torino, Turin, Italy

Ioannis Revolidis Institute for Legal Informatics, Leibniz Universität Hannover, Hannover, Germany

Benjamin Schütze Institute for Legal Informatics, Leibniz Universität Hannover, Hannover, Germany

Jonathan Stoklas Institute for Legal Informatics, Leibniz Universität Hannover, Hannover, Germany

Christine Storr Faculty of Law, Stockholm University, Stockholm, Sweden

Pam Storr Legal Consultant and Teacher in IT law, Stockholm, Sweden

Shinto Teramoto Graduate School of Law, Kyushu University, Fukuoka, Japan

Acronyms

AA	Artificial Agents
AEPD	Agencia Española de Protección de Datos
AIOTI	Alliance for the Internet of Things Innovation
AML	Anti-Money Laundering
ASX	Australia Securities Exchange
BKA	Federal Criminal Police Office (in German: Bundeskriminalamt)
BKAG	Law on the Federal Criminal Police Office (in German: Bundeskriminalamtgesetz)
BSA	Bank Secrecy Act
BSCA	Bank Service Companies Act
C4	CryptoCurrency Certification Consortium
CA	Consortium Agreement
CBS	Cloud Brokerage Scenarios
CDA	Communications Decency Act
CEOs	Chief Executive Officers
CFPB	Consumer Financial Protection Bureau
CIOs	Chief Information Officers
CIOMS	Council for International Organizations of Medical Sciences
CJEU	Court of Justice of the European Union
CoE	Council of Europe
CPDT	Cloud Provider Description Template
CPU	Central Processing Unit
CSS	Cascading Style Sheets Technology
DDoS	Distributed Denial-of-Service
DLT	Distributed Ledger Technology
DMCA	Digital Millennium Copyright Act
DNS	Domain Name System
DPA	Data Protection Authority
DPD	EU Data Protection Directive
DPI	Deep Packet Inspection

DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DRM	Digital Right Management
DSM	EU Commission's Digital Single Market
EASA	European Aviation Safety Agency
ECHR	European Convention on Human Rights
EEA	European Economic Area
ENAC	Italian Civil Aviation Authority
ENISA	European Network and Information Security Agency
EU	European Union
EU GDPR	European Union General Data Protection Regulation
FDIC	Federal Depository Insurance Corporation
FRB	Board of Governors of the Federal Reserve System
GAO	Government Accountability Office
GG	German Constitution (in German: Grundgesetz)
GPS	Global Positioning System
HTTP	Hypertext Transfer Protocol
ICT	Information and Communications Technologies
IDE	Integrated Development Environment
IEEE	Institute of Electrical and Electronics Engineers
IERC	IoT European Research Cluster
IFLA	International Federation of Library Associations and Institutions
IFTTT	If This Then That
IHL	International Humanitarian Law
IMSI	International Mobile Subscriber Identity
IRI	Institute for Legal Informatics
IRS	Internal Revenue Service
ISO	International Standards Organization
ISP(s)	Internet Service Provider(s)
IP	Intellectual Property
IPRs	Intellectual Property Rights
IT	Information Technology
LEAs	Law Enforcement Authorities
MIC	Ministry of Internal Affairs and Communications
MSB	Money Services Business
MTRA	Money Transmitter Regulators Association
NCUA	National Credit Union Administration
NGO	Non-governmental Organization
NIST	US National Institute of Standards and Technology
OCC	Office of the Comptroller of the Currency
OECD	Organization for Economic Co-operation and Development
OGF	Open Grid Forum
OIRA	White House Office of Information and Regulatory Affairs
OTS	Office of Thrift Supervision
PbD	Privacy by Design

PIL	Private International Law
PIPA	Japan's Personal Information Protection Act (Act No. 57 of 2003)
PIPC	Personal Information Protection Commission
PNR	Passenger Name Record
PoF	Points of Failure
QoS	Quality of Service
R&D	Research and Experimental Development
RFID	Radio Frequency Identification
RFO	European Research Funding Organisations
RPO	Research Performing Organisations
RWB	Reporters Without Borders
SaaS	Software as a Service
SCC	Standard Contractual Clauses
SLA(s)	Service Level Agreement(s)
SLO	Service Level Objectives
SMEs	Small and Medium-sized Enterprises
SNS	Social Networking Service
StPO	German Code of Criminal Procedure (in German: Strafprozessordnung)
TFEU	Treaty on the Functioning of the European Union
UK	United Kingdom
UN	United Nations
URL	Uniform Resource Locator
US	United States of America
USD	United States Dollar
VCB	Virtual Currency Business
VC(s)	Venture Capitalist(s)
VM(s)	Virtual Machine(s)
VoIP	Voice over IP
VSG NRW	North Rhine-Westphalia Constitution Protection Act
WHO	World Health Organization
WIPO	World Intellectual Property Organization
WS-Agreement	Web Service Agreement
XML	eXtensible Markup Language
XSD	XML Schema Definition
Y2K	Year 2000

List of Figures

Internet of Things: Right to Data from a European Perspective

Intermediaries and Mutual Trust: The Role of Social Capital in Facilitating Innovation and Creativity

Nudging Cloud Providers: Improving Cloud Architectures Through Intermediary Services

A Brokering Framework for Assessing Legal Risks in Big Data and the Cloud

Disruptive Technologies Shaping the Law of the Future

Marcelo Corrales, Mark Fenwick and Nikolaus Forgó

Abstract Technology is transforming our lives and the way we perceive reality so quickly that we are often unaware of its effects on the relationship between law and society. As an emerging field, a key aim of IT Law is finding the best way of harnessing different cutting-edge technologies and at the same time reducing the ever-growing gap between new technology and various legal systems. Therefore, this chapter deals with introducing and describing several limiting legal issues that have been exacerbated by emerging technologies and the Internet's fast growing and dynamic nature. It follows from this chapter that we could expect disruptive technology and innovation to be integral components to the analysis of law in the future.

Keywords IT Law · Disruptive Technology · Big Data · Cloud Computing · Artificial Intelligence (AI)

Contents

M. Corrales (✉) · N. Forgó
Institute for Legal Informatics, Leibniz Universität Hannover, Hannover, Germany
e-mail: marcelo.corrales13@gmail.com

M. Fenwick
Graduate School of Law, Kyushu University, Fukuoka, Japan

M. Corrales et al. (eds.), *New Technology, Big Data and the Law*,
Perspectives in Law, Business and Innovation, DOI 10.1007/978-981-10-5038-1_1

1 Introduction

Information technology law (or IT Law) is a young field, which was practically unknown just a few decades ago. It goes back, however, to an era before personal computers entered mainstream markets.[1] However, it was not until the mid-1990s and the advent of the Internet that the union of the fields of IT and Law into a unified system became more apparent.

The social and technological context driving this academic development has been the extraordinary growth, over the last decade, in opportunities for companies and organizations to store, transfer and share data over the Internet. The expansion and upsurge of pervasive technologies,[2] which provide new online services, often create legal ambiguities and unprecedented new legal problems.

This collection takes up various new technologies that are currently shaping the law. Such technologies include Cloud computing, Big Data, the Internet of Things (IoT), artificial intelligence (AI), cryptography, sensors, robots, algorithms and other information related systems.

Most of these technologies depend on Cloud computing infrastructures to operate at the upper level. The term "Cloud computing"[3] can be, in some ways, seen as just a metaphor that represents the Internet. It was mentioned by Eric Schmidt in the year 2006 when he was referring to software as a service (SaaS): "You never visit them; you never see them. But they are out there. They are in a Cloud somewhere. They are in the sky, and they are always around. That's roughly the metaphor."[4]

The Cloud has been perceived as one of the most disruptive technologies over the last twenty years.[5] According to a prediction from *CISCO*, by 2020, one-third of *all* data will be stored in or transferred through the Cloud.[6] The Internet world as we know it today is transforming into an "everything-as-a-service"[7] and Cloud services are the building blocks for this change.[8] This is in line with the predictions of leading scientist in theoretical physics, Michio Kaku, who has stated: "Computers as we now know them will disappear; they will be everywhere and nowhere,

[1]Lodder and Oskamp (eds) (2006), pp. 3–4.

[2]Lloyd (2014), p. 5.

[3]The term Cloud computing has been defined in various ways. The US National Institute of Standards and Technology (NIST) provides one of the best definitions as it embraces important aspects of the Cloud. This definition is meant to serve as a comparative model of the different Cloud services and deployment services: "Cloud computing is a model for enabling 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." See Mell and Grance (2011), pp. 1–2.

[4]The work of Eric Schmidt, see Lindberg and Svensson (2010), p. 13.

[5]Garthwaite (2014).

[6]Bort (2011).

[7]For details, see Radenkovie and Kocovic (2014), p. 6.

[8]See, e.g., McKendrick (2016).

ubiquitous yet hidden, just like electricity and running water. The Cloud will follow us silently and seamlessly, carrying out our wishes anytime, anywhere."[9]

Big Data is another disruptive technology that stands at the center of this book. Big Data utilizes a Cloud infrastructure and has brought new and complex ways of processing and analyzing information at a larger scale.[10] This term can be loosely described as "data that exceeds the processing capacity of conventional database systems."[11] The size of data is so large that it surpasses the architecture of a standard database found in a conventional personal computer. It refers, however, not only to the massive amounts of data, but also encompasses all the methods and processes that result in information that support the analyses of science and business decision-making.[12]

IoT is another trend and technological buzzword of the last decade, which is also central to this work. IoT embraces a new concept in which the ubiquitous and virtual world of the Internet converges with the everyday world of "things." The idea is to connect not only people with each other, but also people with everyday devices and items. The term was first coined by the *Auto-ID Center* and after that it has been widely used as term in the research community and computing market.[13]

There is no doubt that all these new technologies are changing the scope in which law is designed, interpreted and applied in a constantly evolving environment.[14] There is, therefore, an increasing global awareness that the traditional concepts and approaches to legal science must be expanded to encompass new areas associated with networked technologies, automation and information science.[15] Based on this new reality, this work aims to provide insights on some of the key legal topics that affect our daily lives. The aim is to answer some of these questions from an inter-disciplinary point of view taking into account a variety of legal systems, including the US, the EU and Japan.

2 Parts

This collection reveals the multi-disciplinary and dynamic character of contemporary IT Law. As such, the book chapters have been divided into three "parts." *Part I* has data protection and privacy issues as its overarching subject, and discusses the different approaches in the EU and Japan. *Part II* discusses the crucial role of *intermediaries* on the Internet, and in the technology field more generally,

[9]Kaku (2013).

[10]For details, see Chen et al. (2014), pp. 12 et seq.

[11]Dumbill (2012), Chapter 2.

[12]Kalyvas (2015), p. 1.

[13]See Uckelmann et al. (2011), pp. 1–2.

[14]Cyrul (2014), Preface.

[15]Council of Europe (1994), p. 9.

and asks how such actors can assist in the innovation process. Finally, *Part III* deals with various technologies that facilitate the gathering of legal evidence and support law enforcement.

The chapters cut across a number of conventional fields and related sub-fields of law, including E-Commerce, data protection, data security and intellectual property. In addition, the chapters also focus on the theoretical foundations of the various issues, based on theories that traditionally fall under the general headings of legal philosophy, law and economics, and behavioral law and economics.

2.1 Purpose and Limitation

One of the key aspects of IT Law has been focused on solving privacy and data protection issues.[16] The rapid growth and proliferation of the Internet, in particular the ease and speed of communications raised problems for companies and organizations when they use, transfer and share data across multiple jurisdictions. Any kind of data outsourcing represents a legal risk.[17] Legislation analyzed in the chapters of this section are mostly based on the European General Data Protection Regulation[18] (EU GDPR), which entered into force in May 2016, and the Japanese Act on the Protection of Personal Information[19] (Japanese Act), which was promulgated on 9 September 2015 and is expected to come fully in force by September 2017. Both regulations attempt to strengthen the data protection regime by granting individuals more control over their data when using Internet services.

The EU GDPR has been generally well received for updating some of the rules in the previous EU Data Protection Directive.[20] However, it has also generated a lot of concerns with regard to its practicability and flexibility to modern data processing technologies, such as Cloud computing, Big Data and IoT. Similarly, substantial amendments have been made to the Japanese Act. These new provisions generally increased the burden and responsibilities on data controllers and place new limitations on exporting personal data to overseas countries.

[16]See, e.g., Barnitzke et al. (2011).

[17]See, e.g., Djemame et al. (2012).

[18]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). While the Regulation entered into force on 24 May 2016, it shall apply to all EU Member States from 25 May 2018. See European Commission, Reform of EU Data Protection Rules http://ec.europa.eu/justice/data-protection/reform/index_en.htm. Accessed 10 October 2016.

[19]Act No. 57 of 2003.

[20]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.

This part will seek to identify some of the complexities and salient points that may be witnessed when applying the data export rules contained in both the EU GDPR and the Japanese Act in Cloud computing, Big Data and IoT scenarios. As constant data transfers are key components of Cloud technology,[21] it is encouraging that certain provisions in the EU GDPR and the amendments to the Japanese Act will facilitate this. Nevertheless, it is also necessary to iron out the missing issues, as will be further outlined in this part.[22]

2.2 *Innovation Intermediaries*

This part discusses the crucial issue of inter-mediation and the role of intermediaries that affect the legal environment for innovation process and economic growth. The concept of the "innovation intermediary" has been an important element in innovation studies to help us understand the role of governments, commercial firms, agencies and individuals.[23] Such intermediaries have been variously referred to as "brokers," "bridgers," or "change agents," as they form the linchpin that facilitate user innovation and creativity.[24] They may be generically defined as: "an organization that bridges the gap between organizers that seek solutions to an innovation problem and innovators that can provide a solution to an organizer's problem."[25] The number of innovation intermediaries has risen exponentially in recent years since they play a vital role in the distribution and access to complex networks.[26] Besides providing direct links between the actors involved, they ensure fluidity and support for accessing all innovation factors.[27]

The chapters in this part explore and bring together different schools of thought regarding such innovation intermediaries. The first stream is the "*diffusion and technology transfer*" literature, where intermediaries promote and expedite the diffusion of information and uptake of new products or services. In this field, the role of intermediaries is also fundamental for the formation of alliances, facilitating relationships and informal group collaborations, providing negotiation skills and formalizing agreements.[28]

The second stream belongs to the "*innovation management*" literature, which suggests that intermediaries take a more active role beyond the mere brokering or

[21]See, e.g., Kuner (2012), pp. 9 et seq.
[22]Nwankwo (2014), pp. 32–38.
[23]Howells (2006), pp. 715–728.
[24]Stewart and Hyysalo (2008), pp. 295–325.
[25]Hallerstede (2013), p. 35.
[26]Osorio et al. (2012), p. 201; Antikainen (2012), p. 189.
[27]Nauwelaers (2011), p. 474.
[28]Hallerstede (2013), p. 35.

networking. They could be described as "architects" with a strong influence and valuable role in the creation of knowledge in collaborative innovation.[29]

Finally, the third stream belongs to the "*systems and networks*" literature, which takes a much broader view on innovation intermediaries and suggests their strong influence as the new drivers on the overall innovation system and policy framework. This strand holds the view that intermediaries (or brokers) link the key players in the market by orchestrating the system on a much deeper and strategic level. They also build up close interactions and continuous communication with their clients producing high added value products and services.[30]

The fundamental insight of these three strands is that by improving the resources and capabilities of the firms, innovation intermediaries are—albeit in an indirect way—facilitating market development.[31] The primary focus is on their core role in configuring, managing and brokering new technologies[32] and services in emerging Internet trends.

2.3 Digital Evidence

The proposal of this part attempts to target a wider audience and includes legal and ethical analysis of various cutting-edge technologies such as AI and robotics. The topics range from cryptography and fragmentation of data to the most advanced safety standards and techniques that serve as legal and digital evidence appropriate for the Internet framework. Moreover, the chapters also refer to various issues related to network effects as well as the capital requirements of financial institutions which might be better understood using AI.

The study of AI is often said to have started in 1956 at Dartmouth College in Hanover, New Hampshire. Originally the concept of AI was conceived as "a set of algorithms to process symbols."[33] This initiative led to numerous advances and applications very useful in the field of the Internet, as well as robotics. This includes several computing and electronic devices such as search engines, consumer electronics, automobiles, and various kinds of sensors and algorithms.[34]

By and large, AI focuses on certain aspects or specialized "intelligent" capabilities of various computing systems, which is now expanding to other areas for the study of the human brain and body and the interrelation with its environment. This is revolutionizing our way of thinking that goes beyond its original conception. For example, it provides useful information for analyzing corporations, groups of

[29]Agogué et al. (2012), pp. 1–31; Hallerstede (2013), p. 36.

[30]Hallerstede (2013), p. 37.

[31]Dalziel and Parjanen (2012), p. 120.

[32]See, e.g., Stewart and Hyysalo (2008), pp. 295–325.

[33]Lungarella et al. (2007), p. 1.

[34]Lungarella et al. (2007), p. 1.

agents and network embedded systems.[35] Nonetheless, these technologies are also surrounded by all kinds of risks, threats, challenges and legal concerns, particularly in the process of gathering digital evidence and law enforcement.

Another novel technology analyzed in this part refers to "crypto-currencies," which follows the principles underlying the decentralized cryptographic technology that enables the "Blockchain."[36] Blockchain is the verification system behind Bitcoin that allows people who do not know (or trust) each other to build a large digital record of "who owns what" that will enforce the consent of everyone concerned.[37] The Blockchain "acts as a consistent transaction history on which all 'nodes' eventually agree."[38] It is essentially a public ledger with the potential to store and transfer tangible assets (physical properties such as cars, real estate property, etc.) and intangible assets (such as votes, genomic data, reputation, intention, information, software and even ideas).[39] In other words, the Blockchain allows the parties to send, receive and store value or information through a distributed peer-to-peer network of several computers.[40]

Each transaction is distributed across the entire network and is recorded on a block only when the rest of the network ratifies the validity of the transaction based on past transactions taking into account the previous blocks.[41] Each block follows the other one successively and this is what "creates" the Blockchain. Each block contains a unique fingerprint using cryptographic hash codes techniques to secure authentication similar to those used in electronic signatures.[42]

If we take Bitcoin[43] as an example, the "coins" themselves are neither physical assets, nor even digital files, but entries in a public ledger using its own unit of account. Therefore, owning a Bitcoin is more like a declaration of owning something, which is recorded on the Blockchain.[44] The distributed nature of this technological model has profound implications in the decentralization of the financial system where traditional intermediary authorities (such as banks or governmental institutions) might no longer be needed.[45]

---

[35]See Lungarella et al. (2007), p. 1; Wang and Goertel (eds) (2007), p. 1.

[36]On 31 October 2015, The Economist featured the "blockchain" on its front cover page: "*The Trust Machine: How the technology behind Bitcoin could change the world.*" For details, see The Economist (2015a).

[37]For details, see The Economist (2015b).

[38]Wattenhofer (2016), p. 85.

[39]Swan (2015), p. 16.

[40]Kost de Sevres (2016).

[41]Kost de Sevres (2016).

[42]Mougayar (2015).

[43]For details, see Hoegner (ed) (2015).

[44]For details, see The Economist (2015c).

[45]Huang (2015), p. 3.

3 Chapters

The book comprises eleven substantive chapters.

Part I—*Purpose and Limitations*—consists of four contributions.

Nikolaus Forgó, Stefanie Hänold, and *Benjamin Schütze* explore the principle of purpose limitation in the context of Big Data. Although Big Data can be enormously useful for better decision-making and risk or cost reduction, it also creates new legal challenges. Especially where personal data is processed in Big Data applications, such methods need to be reconciled with data protection laws and principles. Such principles need constant analysis and refinement in the light of technical developments. Particularly challenging in that respect is the key principle of purpose limitation. It provides that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. This may be difficult to achieve in Big Data scenarios. When personal data is collected, it may be unclear for what purpose it will later be analyzed. However, the blunt statement that the data is collected for any possible Big Data analytics is clearly not a sufficiently specified purpose. Therefore, this chapter further examines the principle of purpose limitation in European data protection law in the context of Big Data applications in order to reveal legal obstacles and possible lawful means for dealing with this issue.

Cecilia Magnusson Sjöberg retains a focus on data protection in an EU context in her discussion of research and academic e-learning. Research and education are major activities in our society, and digitalization has become a fundamental aspect of developments in these fields. In particular, internationalization is a core characteristic of contemporary science. Moreover, knowledge that emerges from the research community evidently serves as the basis for many other disciplines. Education, based on scientific findings and not opinions, is just one example. This, in turn, requires an infrastructure that allows for digitalization both with regard to research in itself but also for the purpose of learning. This topic area is narrowed down to an investigation into current legal developments with regard to data protection for privacy purposes in the context of research and e-learning, bearing academic freedom in mind. The analysis is carried out in the context of the EU's legal framework for data protection.

Christine Storr and *Pam Storr* focus on data protection in the context of the Internet of Things. The starting point of their chapter is the fact that the amount of data collected and processed by "smart" objects has increased exponentially over recent years. The use of this technology, the Internet of Things, leads to various new challenges and applications of existing data protection laws. Data resulting from the use of such technology clearly has wide-ranging consequences for individual privacy, as a large amount of the data in question is often personal in nature. However, the Internet of Things has a wider impact and creates questions within such fields as contract law and intellectual property law, due in large part to the lack of a clear property right to data. In addition, issues of data security are of

importance when such technology is used, particularly when considering liability for data loss. This chapter explores some of the legal issues connected to the Internet of Things from a European perspective, taking into account existing laws and in light of the new European Data Protection Regulation. The underlying theme of the chapter focuses on the existence of legal rights to data created through the use of the Internet of Things and the various actors that may have an interest in the data, from the service provider and the individual user, to intermediaries and those involved in allowing smart objects to fulfill their potential.

Yuriko Haga discusses the right to be forgotten from a comparative perspective, examining European and Japanese developments. The right to be forgotten might be seen as a new right proposed in the context of the emerging information society. Reactions to this right vary from country to country, since the concept remains fluid. The starting point of the argumentation here is to ask whether the right to be forgotten is a part of the right of privacy or totally new and different right. In spite of some differences, the chapter argues that the right should be deemed an extension of privacy. However, because understanding on the concept of privacy itself is not harmonized, there is a tension amongst countries, most obviously between Europe and the US. This chapter explores this issue in the context of the Japanese experience, particularly recent Japanese case-law on the right to be forgotten. The chapter argues that an analysis on the right to be forgotten can help clarify a number of unresolved questions on privacy and that, in doing so, it becomes necessary to modify the general theory itself.

Part II—Innovation Intermediaries—comprises four chapters.

Shinto Teramoto and *Paulius Jurčys* discuss information intermediaries and mutual trust, focusing on the role of social capital in facilitating innovation and creativity. The chapter starts by considering the idea of the role IP rights play in promoting innovation. Recently, however, such a common opinion has been increasingly criticized arguing that IP rights often create more hurdles to innovation than add stimulus. This chapter begins by providing a critical account of the role of IP rights and rules governing unfair competition as legal tools that are supposed to stifle innovation. Acknowledging the significance of IP rights and competition law, this chapter points out that the prevailing theories of IP rights do not provide a clear-cut explanation about the origins of creativity, innovation and the reasons why people engage in creative activities.

The chapter shows that besides IP rights, multiple other factors and policy measures contribute to creativity and innovation. In particular, it is suggested that the success of collaboration in creative endeavors very much depends on the dynamics of interpersonal relations and mutual trust among creators, as well as other participants in the innovation ecosystem. Individuals who trust each other are more likely to come up with creative ideas and materialize them. The chapter aims to contribute to the debate and discusses the role of intermediaries who play a key role in disseminating information. A closer look to changes in the publishing business illustrates that non-legal factors such as mutual trust help reduce transaction costs and open new opportunities to share information. This chapter offers

some considerations about the possible improvements of the legal framework to help promote the accumulation of social capital and creativity. The main claim of the chapter is that the legal system should be more amenable to creators' choices in building new frameworks of collaboration and dissemination of information.

In their chapter, *Marcelo Corrales and George Kousiouris* examine the issue of how Cloud architecture can be improved via intermediary services. The starting points are the uncertainties surrounding the failure of Cloud service providers to clearly assert "ownership" rights of data during Cloud computing transactions. Big Data services have thus been perceived as imposing transaction costs and slowing down the Internet market's ability to thrive.

The novel contribution of this chapter is the development of a new contractual model advocating the extension of the negotiation capabilities of Cloud customers, through an automated and machine-readable framework, orchestrated by a Cloud broker. In doing so, this chapter situates theories of behavioral law and economics in the context of Cloud computing and Big Data, and takes "ownership" rights of data as a canonical example to represent the problem of collecting and sharing data at the global scale. The chapter highlights the legal constraints concerning the Japan's Personal Information Protection Act (Act No. 57 of 2003) and proposes to find a solution outside the boundaries and limitations of the law. By allowing Cloud brokers to establish themselves in the market as entities coordinating and actively engaging in the negotiation of Service Level Agreements (SLAs), individual customers, as well as Small and Medium-sized Enterprises (SMEs), could efficiently and effortlessly choose a Cloud provider that best suits their needs. This can yield new results for the development of Cloud computing and the Big Data market.

Marcelo Corrales and Karim Djemame propose a brokering framework for assessing legal risks in a Cloud-Big Data setting. After decades in which individuals and companies used to host their data and applications using their own IT infrastructure, the world has seen the stunning transformation of the Internet. Major shifts occurred when these infrastructures began to be outsourced to public Cloud providers to match commercial expectations. Storing, sharing and transferring data and databases over the Internet is convenient, yet legal risks cannot be eliminated. Legal risk is a fast-growing area of research and covers various aspects of law. Current studies and research on Cloud computing legal risk assessment have been, however, limited in scope and focused mainly on security and privacy aspects. There is little systematic research on the risks, threats and impact of the legal issues inherent to database rights and "ownership" rights of data. Database rights seem to be outdated and there is a significant gap in the scientific literature when it comes to the understanding of how to apply its provisions in the Big Data era. This means that we need a whole new framework for understanding, protecting and sharing data in the Cloud. The scheme proposed in this chapter is based on a risk assessment-brokering framework that works side by side with SLAs. This proposed framework will provide better control for Cloud users and will go a long way to increase confidence and reinforce trust in Cloud computing transactions.

Ioannis Revolidis discusses Internet intermediaries and copyright, in an EU context. Ever since the commercialization of the Internet the role of Internet

intermediaries has become of vital importance for the functioning of the globalized electronic market and the innovation technologies of information dissemination in general. The importance of the role of the Internet intermediaries has been reflected in the basic legislative initiatives regarding the Internet worldwide. In Europe, following the example of the Communications Decency Act (CDA) and Digital Millennium Copyright Act (DMCA) in the United States, Articles 12–15 of the E-Commerce Directive aimed to create an immunity regime that would allow Internet intermediaries to develop their activities without being hindered by the fear of complex liability issues connected with their sensitive role. At the same time, however, it became apparent that Internet intermediaries are playing a pivotal role in the protection of intellectual property rights in an online world, as they are in the best position to either prevent or bring intellectual property infringements to an end.

This observation was also reflected in the EU legislation, as Articles 12, 13 and 14 of the E-Commerce Directive, Article 8 of the InfoSoc Directive and Article 9 and 11 of the Enforcement Directive provide for a series of interim measures that allow legal action against Internet intermediaries for alleged copyright infringements by third parties. This chapter first highlights what are the current patterns dictated by the case law of the Court of Justice of the EU (CJEU) regarding the role of Internet intermediaries in the enforcement of intellectual property rights and then attempts to assess whether these patterns correspond to the legislative motives and purposes behind the respective EU legislation.

Part III of the book—*Digital Evidence and Law Enforcement*—contains three contributions.

Nikolaus Forgó, Christian Hawellek, Friederike Knoke, and *Jonathan Stoklas* focus on the collection of electronic evidence in Germany. The radical change in telecommunications technologies over the last fifteen years has enabled new techniques to lawfully intercept telecommunications and to gather digital evidence, including covert remote access to data storages and lawful interception prior to communication encryption by hidden software tools. The intrusiveness of these measures, specifically their impact on fundamental rights, have been reflected in recent decisions of the German Federal Constitutional Court dealing with the development of a fundamental right to the integrity and confidentiality of IT systems and limits on covert surveillance measures.

The German legal system is characterized by a strict and fundamental distinction between preventive measures (such as crime prevention) and investigative measures (such as criminal investigation). The distinction results in different legal competences of (police) authorities and a distinct legal framework following an altered proportionality assessment. As a result, the safeguards, checks and balances for investigative measures need to be at least as high as those for preventive measures, requiring corresponding amendments of the Code of Criminal Procedure.

It is therefore surprising to find that the Code of Criminal Procedure governing investigative measures has only undergone minor amendments, such as the introduction of a provision governing the use of International Mobile Subscriber Identity catchers (IMSI catchers). This lack of modernization of the rules applicable to

criminal investigation appears unfortunate, as the measures in question in the view of the chapter's authors should not be based upon the traditional rules designed for physical wire-tapping of telephone lines. Rather, the specific safeguards, such as the requirement to automatically undo alterations imposed upon the infiltrated system, should be codified for investigative measures as well to maintain a comparable level of protection of fundamental rights.

Ugo Pagallo discusses AI, specifically the normative challenges of artificial intelligence and robotics through secondary rules of law. A considerable number of studies have been devoted over the past years, to stress risks, threats and challenges brought on by the breath-taking advancements of technology in the fields of AI and robotics. The aim of this chapter is to address this set of risks, threats, and challenges, from a threefold legal perspective. First, focus is on the aim of the law to govern the process of technological innovation, and the different ways or techniques to attain that aim. Second, attention is drawn to matters of legal responsibility, especially in the civilian sector, by taking into account methods of accident control that either cut back on the scale of the activity via, e.g., strict liability rules, or aim to prevent such activities through the precautionary principle. Third, the chapter focuses on the risk of legislation that may hinder research in AI and robotics. Since we are talking about several applications that can provide services useful to the well-being of humans, the aim should be to prevent this threat of legislators making individuals think twice before using or producing AI and robots. The overall idea is to flesh out specific secondary legal rules that allow us to understand what kind of primary legal rules we may need. More particularly, the creation of legally de-regulated, or special, zones for AI and robotics appears a smart way to overcome current deadlocks of the law and to further theoretical frameworks with which we should better appreciate the space of potential systems that avoid undesirable behavior.

The final chapter, by *Daniel Bunge*, explores the issue of the oversight of Fintech companies. In the United States, the regulatory authority of government agencies over financial institutions' third party service providers varies depending on type of financial institution. The Federal Depository Insurance Corporation (FDIC), the Board of Governors of the Federal Reserve System (FRB), and the Office of the Comptroller of the Currency (OCC) may extend their authority over service providers to their supervised institutions. Meanwhile, the National Credit Union Administration (NCUA) lacks this authority for credit unions. The federal and state agencies that oversee Money Service Businesses (MSBs) also lack this authority. The regulatory authority over MSB service providers is particularly interesting because of the rise of virtual currency businesses providing an alternative payment rail outside of traditional institutions, allowing small Fintech startups to enter into the payment space.

This chapter examines federal and state authority over third party service providers and its justifications. It goes on to examine some of the more unique aspects of Fintech entrants to the payment space and how their service providers should be treated along with other MSBs. Ultimately, this chapter recommends that private contract law between MSBs and their service providers should be used to mitigate

the risks in their relationship. Limited resources and duplicative regulatory costs between federal and state agencies as well as the relatively small size of the industry makes it inefficient to directly supervise third party service providers. However, the argument developed here does not exclude the possibility of a future extension of government authority as the industry and its potential impact on the financial system grows.

References

Agogué M, Yström A, Le Masson P (2012) Rethinking the role of intermediaries as an architect of collective exploration and creation of knowledge in open innovation. Int J Innov Manag 7 (2):1–24

Antikainen M (2012) Towards collaborative open innovation communities. In: Chauvel D (ed) Leading issues in innovation research. Academic Publishing International Ltd, Reading

Barnitzke B, Corrales M, Forgó N (2011) Aspectos legales de la computación en la nube: protección de datos y marco general sobre propiedad intelectual en la legislación Europea. Editorial Albremática, Buenos Aires

Bort J (2011) 10 Technologies that will change the world in the next 10 years. NetworkWorld. http://www.networkworld.com/article/2179278/lan-wan/10-technologies-that-will-change-the-world-in-the-next-10-years.html. Accessed 10 Oct 2014

Chen M et al (2014) Big data: related technologies, challenges and future prospects. Springer, Cham

Council of Europe (1994) Teaching, research and training in the field of law and information technology, recommendation no R (92) 15 and explanatory memorandum. Council of Europe Press

Cyrul W (2014) Information technology and the law. Jagiellonian University Press, Krakow

Dalziel M, Parjanen S (2012) Measuring the impact of innovation intermediaries: a case study of Tekes. In: Melkas H, Harmaakorpi V (eds) Practice-based innovation: insights, applications and policy implications. Springer, Berlin

Djemame K et al (2012) Legal issues in the cloud: towards a risk inventory. Philos Trans R Soc A 371(1983):20120075

Dumbill E (2012) Getting up to speed with big data: what is big data? In: O'Reilly Media, big data: current perspectives from O'Reilly Media. O'Reilly Media Inc., Beijing

Garthwaite E (2014) It's official: cloud is the most disruptive force for 20 years. ItProPortal. http://www.itproportal.com/2014/05/12/cloud-most-disruptive-force-for-20-years/. Accessed 10 Oct 2016

Hallerstede S (2013) Managing the lifecycle of open innovation platforms. Springer, Wiesbaden

Hoegner S (ed) (2015) The law of bitcoin. iUniverse, Bloomington

Howells J (2006) Intermediation and the role of intermediaries in innovation. Res Policy 35(5): 715–728

Huang P (2015) A dissection of bitcoin. Lulu.com

Kalyvas J (2015) A big data primer for executives. In: Kalyvas J, Overly M (eds) Big data: a business and legal guide. CRC Press, Boca Ratón

Kaku M (2013) A scientist predicts the future. The New York Times. http://www.nytimes.com/2013/11/28/opinion/kaku-a-scientist-predicts-the-future.html?_r=0. Accessed 10 Oct 2016

Kuner C (2012) The European commission's proposed data protection regulation: a copernican revolution in european data protection law. Bloomberg BNA privacy and security law report. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2162781. Accessed 10 Oct 2016

Kost de Sevres N (2016) The blockchain revolution, smart contracts and financial transactions. https://www.dlapiper.com/en/uk/insights/publications/2016/04/the-blockchain-revolution/. Accessed 10 Oct 2016

Lindberg A, Svensson D (2010) IT law from a practitioner's perspective. In: Wahlgren P (ed) ICT legal issues: scandinavian studies in law, vol 56. Stockholm Institute for Scandinavian Law, Stockholm

Lodder A, Oskamp A (eds) (2006) Information technology and lawyers: advanced technology in the legal domain, from challenges to daily routine. Springer, Dordrecht

Lloyd I (2014) Information technology law, 7th edn. Oxford University Press, Oxford

Lungarella M et al (2007) AI in the 21st century—with historical reflections. In: Lungarella M et al (eds) 50 years of artificial intelligence: essays dedicated to the 50th anniversary of artificial intelligence. Springer, Berlin

McKendrick J (2016) Is all-cloud computing inevitable? Analysts suggest it is. Forbes. http://www.forbes.com/sites/joemckendrick/2016/07/05/is-all-cloud-computing-inevitable-analysts-suggest-it-is/#402342085b4f. Accessed 10 Oct 2016

Mell P, Grance T (2011) The NIST definition of cloud computing. National Institute of Standards and Technology (NIST), U.S. Department of Commerce. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf. Accessed 10 Oct 2016

Mougayar W (2015) Understanding the blockchain: we must be prepared for the blockchain's promise to become a new development environment. O'Reilly. https://www.oreilly.com/ideas/understanding-the-blockchain. Accessed 10 Oct 2016

Nauwelaers C (2011) Intermediaries in regional innovation systems: role and challenges for policy. In: Cooke P et al (eds) Handbook of regional innovation and growth. Edward Elgar Publishing, Cheltenham

Nwankwo IS (2014) Missing links in the proposed EU data protection regulation and cloud computing scenarios: a brief overview. JIPITEC 5:32–38 https://www.jipitec.eu/issues/jipitec-5-1-2014/3905. Accessed 10 Oct 2016

Osorio D, Jiménez M, Arroyo L (2012) Open innovation through intermediaries in the web: a comparative case study. In: de Pablos C, López Berzosa D (eds) Open innovation in firms and public administrations: technologies for value creation. Information Science Reference (IGI Global), Hershey

Radenkovie B, Kocovic P (2014) From mainframe to cloud. In: Despotovic-Zrakic M, Milutinovic V, Belic A (eds) Handbook of research on high performance and cloud computing in scientific research and education. Information Science Reference (IGI Global), Hershey

Stewart J, Hyysalo S (2008) Intermediaries, users and social learning in technological innovation. Int J Innov Manag 12(3):295–325

Swan M (2015) Blockchain: blueprint for a new economy, 1st edn. O'Reilly, Beijing

The Economist (2015a) The trust machine: how the technology behind Bitcoin could change the world. http://www.economist.com/printedition/covers/2015-10-29/ap-e-eu-la-me-na-uk. Accessed 15 Oct 2016

The Economist (2015b) The great chain of being sure about things. http://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable. Accessed 10 Oct 2016

The Economist (2015c) Bitcoin: the next big thing. http://www.economist.com/news/special-report/21650295-or-it-next-big-thing. Accessed 10 Oct 2016

Uckelmann D, Harrison M, Michahelles F (2011) An architectural approach towards the future internet of things. In: Uckelmann D, Harrison M, Michahelles F (eds) Architecting the internet of things. Springer, Berlin

Wang P, Goertel B (eds) (2007) Advances in artificial general intelligence: concepts, architectures and algorithms. In: Proceedings of the AGI workshop 2006. IOS Press, Amsterdam

Wattenhofer R (2016) The science of the blockchain. Printed by CreateSpace (Independent Publishing Platform)

Part I
Purpose and Limitation

The Principle of Purpose Limitation and Big Data

Nikolaus Forgó, Stefanie Hänold and Benjamin Schütze

Abstract In recent years, Big Data has become a dominating trend in information technology. As a buzzword, Big Data refers to the analysis of large data sets in order to find new correlations—for example, to find business or political trends or to prevent crime—and to extract valuable information from large quantities of data. As much as Big Data may be useful for better decision-making and risk or cost reduction, it also creates some legal challenges. Especially where personal data is processed in Big Data applications such methods must be reconciled with data protection laws and principles. Those principles need some further analysis and refinement in the light of technical developments. Particularly challenging in that respect is the key principle of "purpose limitation." It provides that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. This may be difficult to achieve in Big Data scenarios. At the time personal data is collected, it may still be unclear for what purpose it will later be used. However, the blunt statement that the data is collected for (any possible) Big Data analytics is not a sufficiently specified purpose. Therefore, this contribution seeks to offer a closer analysis of the principle of purpose limitation in European data protection law in the context of Big Data applications in order to reveal legal obstacles and lawful ways to handle such obstacles.

Keywords Big Data · Purpose limitation · Purpose specification · Compatible use · Data protection · General data protection regulation (GDPR) · Data protection directive (DPD)

N. Forgó (✉) · S. Hänold · B. Schütze
Institute for Legal Informatics, Leibniz Universität Hannover, Hannover, Germany
e-mail: forgo@iri.uni-hannover.de

M. Corrales et al. (eds.), *New Technology, Big Data and the Law*,
Perspectives in Law, Business and Innovation, DOI 10.1007/978-981-10-5038-1_2

Contents

1 Introduction

Data, or uninterpreted information, has been collected, stored and processed as long as mankind has existed. Humans have always had a desire to observe and interpret their environment and gather information that would form a solid basis for their decision-making. Yet with the emergence of computers, information technology and digital data processing the game has changed. Since then, the volume of data is growing exponentially and it is expected that by 2020 more than 44 zettabytes (44 Trillion GB) will be generated and approximately 16 zettabytes may be used in the context of Big Data applications.[1] Recent numbers are even more staggering as it is believed that by 2025 the total amount of Data will be as high as 180 zettabytes.[2]

[1] Turner et al. (2014); Cavanillas et al. (2015), p. 3.

[2] Kanellos (2016).

This enormous growth mainly stems from the increasing number of devices generating data, as well as the growing number of built in sensors in each device.[3] More and more devices are connected to the Internet and it is expected that in 2020 nearly 30 billion devices will have an Internet connection.[4] Thus, we find ourselves in an era in which the Internet of Things, i.e., devices communicating with each other, is not a far-fetched dream of the future, but is in the process of happening.

Big Data comes into play when vast amounts of raw data generated by a plethora of different sensors and devices is further stored and processed. It is a challenge for information technology experts to build the pertinent tools to process large quantities of very heterogeneous data, and thus manage this information more effectively. The ability to extract knowledge and value as a result is perceived as a competitive advantage—a future imperative—rather than a luxury. Many organizations, private companies and public institutions alike are expanding their Big Data capabilities and new business models continuously emerge.

However, not only IT professionals are challenged to find solutions for the swelling tide of data. Big Data also poses a considerable number of legal questions and issues of interest for the humanities. Many of them are discussed in research projects such as ABIDA or SoBigData in which the authors of this chapter are (co-) responsible for the legal work package.[5] For example, it is currently legally unclear how far data can be "owned" (in terms of an absolute property right), and if so *who* the owner is.[6] Furthermore, large amounts of data in the hands of one entity raise competition and antitrust law concerns.[7]

One of the most insistent legal challenges of Big Data applications resonates in data protection law, in cases where the data sets processed are to be qualified as personal data. If personal data is processed, then a Big Data provider under the European legal regime has to comply with European data protection law, i.e., the data protection legislation of the European Member States. This legislation was, to some extent, harmonized by the Data Protection Directive (DPD)[8] and will be further modified and reinforced by the European General Data Protection Regulation (GDPR),[9] applicable from May 2018 onwards.

---

[3]Kanellos (2016).

[4]Kanellos (2016).

[5]See http://www.abida.de and http://www.sobigdata.eu/ for further information.

[6]See, e.g., Zech (2012); Grützmacher (2016), pp. 485–495.

[7]See, e.g., Bundeskartellamt, Autorité de la concurrence (2016); Körber (2016), pp. 303–310; pp. 348–356.

[8]European Parliament and the Council (1995) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[9]European Parliament and the Council (2016), 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).

One of the stable bedrock principles in European data protection law is the principle of purpose limitation. This means in general that processing of personal data in the European Union requires a clearly defined purpose at the time of data collection, and that such data cannot be reused for another purpose that is incompatible with the original purpose. This principle may constrain Big Data applications in Europe because one of the methods to leverage value from Big Data is to use data and further processed datasets for different purposes; and to analyze the data in a way that may not have been envisaged at the time the data was first collected.

This chapter is divided into six parts, which examine the principle of purpose limitation in the context of Big Data applications. Following the introduction, Sect. 2 introduces Big Data technology and delineates the problems commonly associated with the processing of personal information. Section 3 explains the basic legal framework of data protection in Europe and briefly sketches the history and development of the purpose limitation principle. Section 4 then analyses the purpose limitation principle further and outlines its interrelationship with other data protection principles in European law. To conclude, Sects. 5 and 6 focus on the new GDPR and assess whether its interpretation of the principle of purpose limitation and pertinent rules will facilitate Big Data application, in contrast to the current legal situation under the DPD. This may determine whether the law helps to induce economic growth or rather, due to a strict interpretation of the limitation of purpose, hamstrings economic activities involving Big Data.

2 Big Data Definition

To understand the context in which the principle of purpose limitation may be relevant, it is useful to explain what Big Data means and, even more importantly, in which (business) environments and value chains it is set. In recent years, the term "Big Data" has been used prolifically. However, until now it remains somewhat obscure what exactly Big Data means and implies. It is not a legal term but rather describes a phenomenon with a multitude of different implications in scientific disciplines, such as economics, technical disciplines, legal and social science, and probably in many further areas of life in the years to come.

Several definitions of the term Big Data have been suggested. The first and best known definition was formulated by *Laney*,[10] who proposed a three-dimensional perspective: the "three Vs" with which he described certain characteristics a Big Data application should have.[11] According to *Laney*, "Big Data is high volume, high **v**elocity, and/or high **v**ariety information assets that require new forms of processing to enable enhanced decision-making, insight discovery and process optimization."[12] "Volume" refers to the amount of data and implies that in Big Data

[10]Laney (2001).

[11]Curry (2015), p. 30.

[12]Laney (2001).

scenarios large amounts of data will be processed. "Variety" on the other hand refers to the range of different types and sources of data. It points to the fact that Big Data infrastructures need to cope with a vast array of different sources as well as a variety of different format and syntactic parameters (e.g., images texts, spreadsheets, database entries) "Velocity" refers to the requirement that, in a Big Data scenario, IT systems need to deal with streams of incoming real time data, for example, real time traffic information or electronic trading. As Big Data applications evolved, further attributes have been suggested of which the most important one is "Veracity." It refers to quality aspects of data, since their accuracy and overall quality may vary greatly. A prediction calculated by Big Data methods may thus be upset by inaccurate raw data.[13]

To understand Big Data and its legal implications it is not necessary to formulate a precise technical or legal definition, but rather to understand the value chains and interdependencies between the entities involved in Big Data ecosystems. To understand the business models and their legal implications one may compartmentalize the data handling into three separate steps, beginning with data acquisition, followed by the actual data processing (i.e., analysis, curation and storage) eventually leading to the use of the results of the Big Data analysis. Every step of such data handling may be associated with certain legal questions and effects.

Data acquisition is the process of gathering and filtering raw data before they are stored and further processed. Data can be gathered from ever increasing sensor networks in the so-called Internet of Things (IoT), acquired on online marketplaces or collected from natural persons in social media or via their smartphones, wearables and other mobile devices. The process of acquisition thus raises questions of data ownership as well as data protection, if personal information is collected. Furthermore, data acquisition raises questions of contractual relations if the data is sold and bought including the rights of the buyer in case of breach of contract following the delivery of defective data, i.e., data that is inaccurate or of lower quality than the parties have agreed upon.

The second phase that follows data acquisition is Big Data sensu stricto because only here data is merged and further processed in order to generate new insights. Although it also involves data curation and storage, more important is the actual analysis of the data by exploring and modeling data in order to highlight and extract information relevant for business or other domain-specific decisions. Merging and combining data to gain new insights may have repercussions in data protection law, as it may be that the envisaged merging and analysis is not compatible with the specified purpose articulated at the time of the collection. Or it may be that non-personal information through combining it with other information becomes personal information, because through such newly extracted data a natural person can be identified. Aside from data protection, the process of data curation and storage may also raise questions of data quality as data must be processed in such a way that it is trustworthy, accessible and in general fits the purpose for which it is cured and stored.

[13]An overview of the different Big Data definitions can be found in Curry (2015), p. 31.

The third phase of a Big Data processing scenario is represented by the usage of the results of the analysis and probably is the most significant phase in a Big Data scenario. Data usage covers a wide range of data driven activities and relies on the access to data and the results of a Big Data analysis. In other words, it is the decision-making process, which is based on the result of the Big Data analysis. This may be a "conscious" decision taken by a natural person, however, Big Data will in the future increasingly result in automated decision-making, where autonomous machines carry out certain tasks without human intervention.

Examples of such machines are robots in autonomous factories that are connected to logistic networks and independently order supplies or manage their repairs and upgrades. Manufacturing and logistics are currently undergoing an industry-wide transformation as part of the so-called "Industry 4.0." The term describes the digitization and interconnection of products, manufacturing facilities, and transport infrastructure for purposes such as supply chain management and maintenance. Industry 4.0 corresponds with Big Data, as a precondition for proper management of the decision-making process is to analyze huge amounts of (real time) data. An even more practical example is the self-driving car or other autonomous vehicles. Driverless cars need to be capable of sensing their environment and navigating without human input. This is only possible through an adequate number of sensors with which the car can detect its surroundings. If the self-driving car is to be embedded in a smart traffic scenario, it must further be capable of receiving live traffic data on congestion, road conditions, etc., to calculate the optimal route or travel speed. In order to navigate in traffic, the self-driving car therefore requires Big Data capabilities. In other words, Big Data is a precondition to operate autonomous vehicles, as the on-board computer has to process large amounts of data in a short period of time to navigate safely and predict potentially dangerous traffic situations and react to unforeseen events.

Events that may occur in connection with data usage raise numerous legal questions. However, the following part of the chapter will focus on the aspects of the protection of personal information and, in particular, the principle of purpose limitation.

3 The Development of the Principle of Purpose Limitation

The principle of purpose limitation has served as a key principle and stable element in European data protection law for many years.[14] To understand how it has evolved from the early instruments on human rights and data protection to the most recently enacted GDPR, a brief historical overview is needed. The following section therefore provides a short description of how the concept of purpose limitation came into being, was carved out and redefined.

[14]Article 29 WP, p. 9.

3.1 European Convention on Human Rights (ECHR)

The European Convention on Human Rights was adopted in 1950. Article 8 (1) of the Convention incorporates the right to privacy, according to which everyone shall have the right to respect for his private and family life, his home and his correspondence. Article 8 (2) prohibits any interference by a public authority with the exercise of this right unless such interference is in accordance with the law and necessary in a democratic society to satisfy certain public interests listed in Article 8 (2) ECHR.[15] According to Article 8, any interference with the individual's right to privacy requires justification under strictly defined conditions. Such conditions, and the fact that a legal basis is required forms a starting point for the principle of purpose limitation, as without a legal basis, a legitimate purpose, which at the same time sets limits to the interference, cannot be determined.[16]

3.2 Council of Europe Resolutions (73) 22 and (74) 29

Two important additional steps that should be mentioned are the Council of Europe (CoE) Resolutions (73) 22[17] and (74) 29,[18] which were elaborated further by later instruments and formulated what have become defining principles of data protection law, inter alia, the principle of purpose limitation. Principle 2 CoE Resolution (73) 22 states that, "information should be appropriate and relevant with regard to the purpose for which it has been stored." Furthermore, principle 5 determines that, "without appropriate authorization, information should not be used for purposes other than those for which it has been stored, nor communicated to third parties." CoE Resolution (74) 29, dealing with the protection of privacy in "electronic data banks" in the public sector, reiterates at first, similar to CoE 73 (22), that the information stored should be "appropriate and relevant to the purpose for which it has been stored".[19] Principle 3 (c) goes on to state "that data stored must not be used for purposes other than those which have been defined unless an exception is explicitly permitted by law, is granted by a competent authority or the rules for the

[15]Article 8 (2) ECHR lists national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

[16]Article 29 WP, p. 7.

[17]Council of Europe Committee of Ministers (1973) Resolution (73) 22 on the protection of privacy of individuals vis-à-vis electronic data banks in the private sector, adopted on 26 Sept 1973.

[18]Council of Europe Committee of Ministers (1973) Resolution (74) 29 on the protection of privacy of individuals vis-à-vis electronic data banks in the public sector, adopted on 20 Sept 1974.

[19]Principle 2 (c).

use of the electronic data bank are amended." In other words, 3 (c) introduces the notion that the purpose of information storage may be changed under certain conditions.

3.3 Convention 108

One may say that CoE Resolutions (73) 22 and (74) 29 paved the way for another defining legislative instrument with regard to the principle of purpose limitation: Convention 108 of the Council of Europe.[20] Convention 108 was opened for signatures in January 1981. Article 5 introduces a more elaborate set of data protection principles such as lawfulness, fairness and proportionality. However, three of its five sub clauses refer to key aspects of the principle of purpose limitation. Article 5 (b) determines that personal data undergoing automatic processing shall be "stored for specific and legitimate purposes and not used in a way incompatible with those purposes" (purpose specification). Firstly, this means that it is not permissible to store data for undefined purposes, and it is left to the national legislator, to decide how such purposes must be specified.[21] Secondly it must be emphasized that Article 5 (b) introduces the notion of incompatibility when it determines that the data cannot be used "in a way incompatible" with the specific purposes; this concept has later been incorporated into the Data Protection Directive and General Data Protection Regulation. Article 5 (c) furthermore, addresses the principle of data minimization and determines that personal data must be "adequate, relevant and not excessive in relation to the purpose for which they are stored." In other words, Article 5 (c) connects the principle of data minimization and purpose limitation. Finally, Article 5 (e) interlinks the principle of purpose limitation with anonymization when it determines that "personal information undergoing automatic processing shall be preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored."

Following principle 3 (c) CoE Resolution (74) 29, Article 9 of Convention 108 allows for derogations from Article 5 "when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of: protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences; protecting the data subject or the rights and freedoms of others." Furthermore, Article 9 (3) points, by reverse implication, to another important aspect regarding the principle of purpose limitation. This is that for some purposes, the individual's right to privacy may be restricted, namely when automated personal data files are "used for statistics or for

[20]Council of Europe (1981) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg 28 Jan 1981.

[21]Council of Europe (1981) Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg 28 Jan 1981.

scientific research purposes when there is obviously no risk of an infringement of the privacy of the data subject." Admittedly Article 9 (3) is a slightly different case, as it deals with derogations from Article 8 (b–d) of the Convention. Those require additional safeguards for the data subject such as the right of notification, erasure and rectification. However, it would support the argument that changing the purpose of data storage and processing, as long as it is for statistics or scientific research purposes, is less likely to be seen as an infringement of the privacy of the data subject and not incompatible with the specified and legitimate purposes for which personal data has been stored in the first place.

3.4 OECD Guidelines

The OECD Guidelines[22] governing the Protection of Privacy and Transborder Flows of Personal Data, which were adopted in 1980—almost at the same time Convention 108 was signed—have a similar approach to the purpose limitation principle, but are more specific on the exact time at which the purpose must be specified. Paragraph 9 states that the "purposes for which personal data are collected should be specified not later than at the time of data collection." Furthermore, the Guidelines also incorporate the notion of incompatibility when they state that "the subsequent use should be limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose." Finally, Paragraph 10 explicitly mentions two exceptions to Article 9, determining that use of personal data for purposes other than those specified in accordance with Paragraph 9 may be admissible "with the consent of the data subject" or "by the authority of law." The 2013 review[23] of the OECD Guidelines left these provisions unchanged.

4 The Purpose Limitation Principle Under the Data Protection Directive (DPD) and Its Implications for Big Data Applications

4.1 Starting Position

The Data Protection Directive (DPD) dates back to the year 1995. The DPD was a prominent step to harmonize the data protection rules within the EU. It was the

[22]OECD (1980) Annex to the recommendation of the Council of 23 September 1980: Guidelines governing the protection of privacy and transborder flows of personal data.

[23]OECD (2013) Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data [C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79].

declared aim of the European legislator to remove the obstacles to a free flow of personal data within the EU and at the same time to harmonize the level of protection of the rights and freedoms of individuals with regard to the processing of their personal data.[24] Due to its character as a directive it had to be implemented by the Member States of the European Union into their national legal frameworks.

The European legislator has laid down in Article 6 DPD the basic European data protection law principles, namely the principle of fairness and lawfulness, the purpose limitation principle, the principle of data minimization, the data quality principle and the principle of data security. Referring to the data protection principle of purpose limitation, the Directive determines in Article 6 (1) (b) that personal data must be collected for specified, explicit and legitimate purposes and not be further processed in a manner that is incompatible with these purposes. The specification of the purpose is a core element of the framework established by the Directive. Without specifying the purpose, it is, for instance, not possible to clarify whether the processing is allowed by the applicable data protection regulations. Purpose specification is also necessary in order to determine necessary safeguards for the personal data as well as to fulfill other data protection obligations, such as to inform the data subject of the purposes of the processing of their personal data.[25] In brief, the purpose limitation principle serves two goals. On the one hand, it protects reasonable expectations of data subjects with regard to by whom and how their data shall be processed. On the other hand, it allows data controllers to process data for a new purpose within carefully balanced limits.[26]

4.2 Specified, Explicit and Legitimate Purpose (Purpose Specification)

4.2.1 Purpose Must Be Specified

The first building block of the purpose limitation rule is that the controller, when collecting the data, needs to specify the purpose or purposes, which are intended to be served with the collected data.[27] Purpose specification requires an internal assessment and documentation by the data controller who must clearly and specifically identify the purpose of the collection.[28] This step is elementary for consideration of, and compliance with, other data protection requirements. As already mentioned, Article 6 (1) DPD provides further important data protection principles such as the principle of data minimization, which requires that only

[24]Recital 8 Directive 95/46/EC.
[25]Article 29 WP, p. 15.
[26]Article 29 WP, p. 3.
[27]Article 29 WP, p. 15.
[28]Article 29 WP, p. 15.

personal data is processed, which is adequate, relevant and not excessive in relation to the purposes for which the data are collected and/or further processed. Consequently, the data controller must consider carefully, after specifying the purpose, whether the collection and/or processing of the personal data is necessary for the aim he pursues. In order to support transparency and also to improve enforcement of the purpose limitation principle, data subjects must be informed by the data controller of the purpose of the collection, except where they already have it (Article 10 (b) and Article 11 (b) DPD). This shows that there is a connection between transparency and purpose specification. The transparency aspect enhances predictability for data subjects who know what to expect regarding the processing of their personal data by the data controller.[29]

The rule of purpose limitation would not sufficiently protect the data subjects' rights if it was permissible to use vague or very general descriptions of the envisaged purpose of data processing in order to have a broader scope of manoeuvre.[30] In this regard, the Article 29 Working Party has suggested that purported purpose specifications in such terms as "improving user's experience, marketing purposes, IT-security purposes or future research" are invalid.[31] According to the Article 29 Working Party, the required degree of specification depends on the context in which the data is collected and must be determined for every specific case. In some circumstances simple descriptions of the purpose are appropriate, while others require a more detailed specification.[32] This means in effect that, for example, large retail companies selling goods throughout Europe using complex analytic applications to tailor advertisements and offers to their customers will need to specify the purposes in more detail than a local shop, which is collecting only limited information about their customers.[33] If a data controller provides a number of services (e.g., e-mail, photograph upload, social networking functions) it must ensure users are informed about all the different purposes of the envisaged processing activities.[34] Additionally, if a gaming website service is aimed at teenagers, the age of the respective customer must be taken into account. The same is true for website services targeted at elderly people.[35]

In this context, it is also relevant to mention the limitation of purpose by the data subject by giving her informed consent. National courts,[36] as well as data protection agencies of the Member States,[37] have declared vague and/or blanket forms of

[29]Article 29 WP, p. 13.

[30]Article 29 WP, p. 16; Ehmann and Helfrich (1999), p. 113.

[31]Article 29 WP, p. 16.

[32]Article 29 WP, p. 16.

[33]Article 29 WP, p. 51.

[34]Article 29 WP, p. 51.

[35]Article 29 WP, p. 51.

[36]OLG Frankfurt/M., Judgment 17 Dec 2015—6 U 30/15; LG Berlin, Judgement 19 Nov 2013—15 O 402/12; OLG Celle, Judgement 14 Nov 1979—3 U 92/79.

[37]See, e.g., Metschke and Wellbrock (2002), pp. 27–28.

consent in data processing to be invalid. The subject's informed consent is one of the legal grounds that allows the processing of personal data.[38] Since the limits of the consent given by the data subject also constrain the possibilities of the data controller to process the personal data, this also operates as a mechanism for the data subject to stay in control of the purposes for which her personal data are used. For instance, in the medical research field the data subject cannot give valid informed consent if he is not sufficiently aware of the potential ways in which her personal data may be used. It is, in particular, not possible—when obtaining consent—to refer in a general way to future research projects of which the data subject is unable to form any real idea.[39]

4.2.2 Purpose Must Be Explicit

Another element of the purpose specification building kit is that the purpose specification must be explicit. This means that the specification of the purpose must be clearly disclosed and explained or expressed in an intelligible form. This must happen no later than the time of the collection of the personal data. This requirement contributes to transparency and predictability, as it allows third parties to understand how the personal data can be used and to identify the limits of the processing of the personal data.[40]

4.2.3 Purpose Must Be Legitimate

The purpose for which the data have been collected must be legitimate. This refers in part to the general rules that can be derived from Article 7 and Article 8 DPD, namely that the processing of personal data is prohibited unless there is a legal ground, for example, the consent of the data subject. Moreover, it provides that the purposes must be in accordance with all applicable laws as well as customs, codes of conduct, codes of ethics and contractual arrangements. Finally, the general context and facts of the case may also be considered, for instance, the nature of the relationship between data controller and data subject.[41] Ultimately, the data controller needs to ensure prior to the collection that there is a legal rule allowing the envisaged collection and further envisaged use. Furthermore, they need to take account of other relevant conditions, for example, any civil law obligation they are subject to, or, for instance, in case the data is used in a medical research project,

[38]Article 7 (a) and Article 8 (2) (a) Directive 95/46/EC.

[39]Metschke and Wellbrock (2002), pp. 27–28.

[40]Article 29 WP, p. 17.

[41]Article 29 WP, p. 20.

acknowledged ethical norms such as the Declaration of Helsinki[42] or the International Ethical Guidelines for Epidemiological Studies.[43]

4.3 Assessment of Compatibility

The second building block of the purpose limitation principle is the requirement that the collected data must not be further processed in a way incompatible with the purpose for which the data have been originally collected (compatible use). The Directive does not explicitly state what processing steps fall under further processing; it rather distinguishes between the very first processing, which is the collection of data, and all subsequent processing steps such as storage, analysis etc. Any processing steps following the collection of the personal data are to be seen as further processing of personal data, regardless of whether the processing is for the purpose initially specified or for any additional purpose.[44] By providing that further processing is permitted as long as it is not incompatible, it was acknowledged under the Directive that the European legislator intended to give some flexibility with regard to further use of personal data.[45]

In some cases, it is obvious that further processing is compatible, for example, if the data have been collected to specifically achieve the purpose that shall be achieved with the intended further use. In other cases, the decision whether compatibility can be established or not is not that obvious. The compatibility test must be carefully applied as processing of personal data in a way incompatible with the initially determined purposes is unlawful. The data controller cannot legitimize the further processing that is incompatible with the original purpose simply by relying on a legal ground[46] allowing the processing of the personal data.[47]

The Directive explicitly privileges further processing of personal data for historical, statistical or scientific purposes, provided that Member States implement appropriate safeguards (Article 6 (1) (b) DPD). Under the regime of the Directive it is up to the Member States to specify the appropriate safeguards to satisfy this requirement.[48] These safeguards shall preclude that the data will be used to support

[42]WMA General Assembly (2013) WMA Declaration of Helsinki—Ethical Principles for Medical Research Involving Human Subjects.

[43]Council for International Organizations of Medical Sciences (CIOMS), WHO (2008) International Ethical Guidelines for Biomedical Research Involving Human Subjects.

[44]Article 29 WP, p. 21.

[45]Article 29 WP, p. 21.

[46]National implementations of Article 7 and Article 8 Directive 95/46/EC provide legal grounds for processing personal data.

[47]Article 29 WP, p. 3.

[48]Article 29 WP, p. 28.

or justify measures or decisions against any particular individual (Recital 29 DPD).[49] The Article 29 Working Party has interpreted this requirement very broadly: any relevant impact on particular individuals—either negative or positive—shall be avoided.[50] Appropriate safeguards may be for instance early anonymization, or in cases where the purpose of the processing requires the retention of the information in identifiable form other techniques, for instance, pseudonymizing the personal data and keeping the keys coded or encrypted and stored separately.[51] The privileging rule for further processing for historical, statistical or scientific purposes covers a diversity of processing activities ranging from activities supporting public interests—such as medical research—or purely for commercial purposes, for example, market research.[52] In particular, the exemption for statistical purposes is relevant for Big Data applications that try to find correlations and new trends.

Other forms of further use not covered by the privileging rule in Article 6 (1) (b) of the Directive, are as indicated earlier, not precluded per se; this is only so if they qualify as incompatible with the original purpose.[53] Whether a given further use qualifies as compatible or incompatible will need to be assessed on a case-by-case basis.[54] The Article 29 Working Party has analyzed the legal provisions and practices in the Member States to assess the compatibility of further processing and identified key factors to be considered in the compatibility assessment:[55]

(i) The relationship between the purposes for which the personal data have been collected and the purposes of further processing;
(ii) The context in which the personal data have been collected and the reasonable expectations of the data subjects as to their further use;
(iii) The nature of the personal data and the impact of the further processing on the data subjects;
(iv) The safeguards adopted by the controller to ensure fair processing and to prevent any undue impact on the data subjects.[56]

[49]Beyleveld (2004), p. 9.
[50]Article 29 WP, p. 28.
[51]Article 29 WP, pp. 30–32; Metschke and Wellbrock (2002), p. 16.
[52]Article 29 WP, p. 29.
[53]Article 29 WP, p. 21.
[54]Article 29 WP, p. 21.
[55]Article 29 WP, pp. 23–27.
[56]Article 29 WP, p. 40, e.g., example 15: mobile phone locations help inform traffic calming measures, p. 66.

4.4 Consequences of the Requirements of the Purpose Limitation Principle Established by the DPD for Big Data Applications

What follows from the above is, firstly, that data controllers cannot simply collect and store any accessible data in order to have the possibility to use such data for a purpose that will be defined in the future.[57] The data processor will need to determine a specific purpose at the latest by the time of data collection. The level of detail required is a matter of degree and depends on the individual circumstances. Vague and blanket specification of the purpose will certainly not suffice.[58] Data controllers can use, for example, the Article 29 Working Party Opinion on purpose limitation[59] or national court decisions[60] for guidance on how to specify the purpose. In general, they should consider that the more the data subject is affected by the envisaged processing of her personal data the more detailed the purpose specification should be.[61] However, the data controller must take into account that there are certain legal fields, for instance, medical research, where the required level of specificity is controversial and where different approaches within the Member States exist.[62]

For the purpose specification data, controllers should determine the types of personal data that are going to be processed, the quantity of the data and also the kind of data they envisage to link with the personal data for the envisaged Big Data application. Possible usage context must be described and—in case the data shall be transferred to third parties—those should be specified, too.[63] This excludes the specification of generic purposes as, for instance, processing of the data for strategy development.[64] Companies need to question the function and the objective of

[57]Werkmeister and Brandt (2016), p. 237.

[58]Article 29 WP, p. 16.

[59]Annex 3 of the Article 29 WP Opinion 03/2013 on purpose limitation gives a number of examples to illustrate purpose specification.

[60]OLG Frankfurt/M., Judgment 17 Dec 2015-6 U 30/15; LG Berlin, Judgement 19 Nov 2013–15 O 402/12; OLG Celle, Judgement 14 Nov 1979—3 U 92/79.

[61]Bretthauer (2016), p. 272; Wolff (2016) margin number 19.

[62]In the UK, broad consent is accepted in some instances (MRC 2011, p. 6). The legal situation in Germany is still unsettled in this regard. German courts (e.g., OLG Celle, Judgement 14 Nov 1979—3 U 92/79) have viewed the use of a broader forms of consent critically in non-medical fields of peronal data processing and it is unsure how this will be translated in medical research. The Data Protection Authorities of the Land Berlin and the Land Hessen seem not to require a consent restricted to a particular research project, but the data subject must be able to gain an idea for what research projects his data will be used for (see Metschke and Wellbrock 2002, p. 27). The working group "Biobanking" published a model broad consent form for biobanks based on recommendations of the National/German Ethics Council (Arbeitskreis Medizinischer Ethikkommissionen in der Bundesrepublik Deutschland e.V. (2013)).

[63]Bretthauer (2016), p. 272; Wolff (2016) margin number 20.

[64]Bretthauer (2016), p. 272.

envisaged Big Data applications in more detail.[65] Open ended Big Data applications where the analysis gives answers to questions that have not been asked before face certain limits here.[66] In order to be in compliance with data protection rules in such cases anonymization of the data may be an option[67] although it also needs to be said that anonymization becomes increasingly difficult in Big Data scenarios due to risks of reidentifiability.

The purpose limitation principle may set another barrier to conduct: Big Data applications as a further processing of the personal data must not be incompatible with the original purpose for which the data was collected. This depends on the individual circumstances. In case the privileging rule for further processing for historical, statistical or scientific purposes does not apply, a compatibility assessment must be conducted. It seems advisable to consider the criteria identified by the Article 29 Working Party as well as the practical examples elaborated on in Annex 3 of the Opinion. The Article 29 Working Party addresses the issue of repurposing data for Big Data analytics.[68] The opinion describes two kinds of further processing relevant for Big Data applications: (1) performing the analysis to detect trends or correlations; or (2) gaining information about certain individuals and making decisions affecting such individuals.[69] The first scenario may pose no further obstacles if appropriate safeguards for the individual's privacy are provided; in the second scenario "free, specific, informed and unambiguous 'opt-in' consent would almost always be required, though, otherwise the further use cannot be considered compatible."[70] For its part, the UK Information Commissioner's Office (ICO) has suggested broadly that a key factor in deciding whether a new purpose is incompatible with the original purpose is whether the further processing can be regarded as fair.[71]

When the purpose for which the data has been collected or further used is fulfilled the data must not be kept for longer in a form, which permits identification of data subjects (Article 6 (1) (e) DPD). Consequently, in such cases, further storage of personal data in order to use them for further analysis that will only be defined in the future is not permitted. However, if appropriate safeguards are provided by the Member States, the personal data can be stored for longer periods for historical, statistical or scientific use (Article 6 (1) (e) DPD. National implementations of this provision facilitate storage of personal data sets that could be used in the future for Big Data analysis which is a supplement to the privileging rule in Article 6 (1) (b) DPD.

[65]Handelsblatt Research Institute (2014), p. 14.

[66]Handelsblatt Research Institute (2014), p. 14; Martini (2014), p. 7; Roßnagel et al. (2016), p. 123.

[67]Raabe and Wagner (2016), p. 437; Handelsblatt Research Institute (2014), p. 14; Martini (2014), p. 15; Dix (2016), p. 60.

[68]Article 29 WP, pp. 46–47.

[69]Article 29 WP, pp. 46–47.

[70]Article 29 WP, p. 46.

[71]Information Commissioner's Office (2014).

5 New Developments Regarding the Purpose Limitation Principle Under the General Data Protection Regulation and Its Impact on Big Data Applications

5.1 *The General Data Protection Regulation—"A Hybrid of Old and New"*[72]

Continuing differences in the level of data protection between the Member States, which has been evaluated as a danger to the free flow of personal data across the EU, as well as challenges posed by changes in the technological environment and globalization (including the continuously growing scale of collecting and sharing personal data) created impulses for reform, which have led to the enactment of the General Data Protection Regulation.[73] The GDPR shall apply from 25 May 2018 onwards.[74] In contrast to the DPD, the GDPR will be directly applicable in all the Member States. However, it also reserves significant legislative powers to the Member States.[75] The Regulation appears as an "unusual hybrid of old and new."[76] It includes, for example, new rules such as the right to data portability,[77] the "right to be forgotten",[78] and mandatory data breach notifications,[79] and it puts a strong emphasis on privacy by design.[80] But it also reaffirms older principles, such as the requirement of a legal ground to allow processing of personal data, although these also sometimes appear in a new guise.

5.2 *Continuation of the Requirement of Purpose Specification and Compatible Use*

The European legislator has placed the purpose limitation principle in Article 5 (1) (b) GDPR. Article 5 of the Regulation also restates other key principles of data protection, such as the principle of data minimization, in Article 5 (1) (c) GDPR, and the principle of fairness and lawfulness, which now includes the explicit requirement of transparency, in Article 5 (1) (a) GDPR. In Article 5 (1) (b) it is

[72]Mayer-Schönberger and Padova (2016), p. 324.
[73]Recitals 5–9 of Regulation (EU) 2016/679; Mayer-Schönberger and Padova (2016), pp. 323–324.
[74]Article 99 (2) Regulation (EU) 2016/679.
[75]Mayer-Schönberger and Padova (2016), p. 325.
[76]Mayer-Schönberger and Padova (2016), p. 324.
[77]Article 20 Regulation (EU) 2016/679.
[78]Article 17 Regulation (EU) 2016/679.
[79]Article 33 Regulation (EU) 2016/679.
[80]Article 25 Regulation (EU) 2016/679.

further stated that personal data shall be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes." Further processing for archiving purposes in the public interest, scientific or historical research purposes shall in accordance with Article 89 (1) GDPR not be considered incompatible with the initial purpose. This reflects the fact that the two earlier identified main building blocks of the purpose limitation principle established by the Data Protection Directive, namely purpose specification and compatible use, still prevail. There is also a provision in Article 5 (1) (b) GDPR privileging further use for statistical purposes or scientific research.

5.3 *New Aspects with Regard to Purpose Specification*

Regarding the first building block element—the purpose specification requirement—it is interesting to note that the GDPR recognizes in Recital 33 that "it is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection." In consequence, data subjects shall be able to give consent to certain areas of scientific research if ethical standards are observed.[81] This may resolve to a certain degree the long and intensive debate on the permissibility of a broad consent in the medical field,[82] as it indicates that consent sheets can be formulated in such a way that the consent covers a broader range of research, not only specific research questions. This, in return, may also have an effect upon the question how specifically the purpose must be determined in advance by the researcher collecting and analyzing the personal data.

5.4 *Inclusion of the Compatibility Assessment Test into the Legal Text of the GDPR*

Regarding the second building block element—compatible use—the Regulation has become more specific with regard to the question of which secondary uses are to be considered compatible. During the legislative process the purpose limitation principle was heavily debated.[83] While the European Commission had included in its draft a passage, which provided a broad exemption from the requirement of compatibility by allowing further processing by simply identifying a new legal ground

[81]Schaar (2016), pp. 224–225.

[82]See elaborations made in footnote 15.

[83]Werkmeister and Brandt (2016), p. 237.

for the processing,[84] the European Parliament rejected this on grounds of principle.[85] Finally, the European legislative organs found a consensus by retaining the rule that further processing must be compatible (n.b., not identical) with the original purpose. They also agreed to adopt in the legislative text a catalogue of criteria, which are similar to the compatibility test criteria identified by the Article 29 Working Party in its opinion on purpose limitation. Article 6 (4) GDPR provides that when performing the compatibility assessment, the following criteria shall, inter alia,[86] be taken into account:

(i) Any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
(ii) The context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
(iii) The nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;
(iv) The possible consequences of the intended further processing for data subjects;
(v) The existence of appropriate safeguards, which may include encryption or pseudonymization.

Article 6 (4) of the Regulation also states that the data controller can, in a case where they want to further process the data for a new purpose, obtain the data subject's consent.

Perhaps one of the real achievements of the Regulation is that the compatibility assessment test is now part of the legal text of the Regulation, which may improve attentiveness and enforceability. Legal scholars who have investigated how Big Data applications can comply with the requirements of data protection law often put special emphasis on the last criteria mentioned—the existence of appropriate safeguards—as a key provision to legitimize Big Data applications.[87] This corresponds with the view taken by the Article 29 Working Party, which states that effective anonymization of the data can reduce concerns regarding incompatible processing even in case of relatively sensitive data and where data subjects would not expect their data to be further processed.[88] However, the existence of appropriate safeguards is just one criterion to consider. The more specific and restrictive

[84]European Commission (2012) 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) (COM/2012/011 final—2012/0011 (COD)).

[85]Albrecht (2016), p. 36.

[86]This shows that the criteria catalogue is not excluding other appropriate considerations.

[87]Raabe and Wagner (2016), p. 438; Marnau (2016), p. 432.

[88]Article 29 WP, pp. 66–67.

the context of collection, the more limitations may apply to further use.[89] It also needs to be considered that Big Data processing makes it more and more challenging to achieve and preserve anonymity.[90]

5.5 *The New Privileging Rule for Further Processing for Archiving Purposes in the Public Interest, Scientific or Historical Research Purposes or Statistical Purposes*

As mentioned above, Article 5 (1) (b) GDPR, similar to Article 6 (1) (b) DPD, provides that further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes—in accordance with Article 89 (1) GDPR shall not be considered to be incompatible with the initial purposes. Recital 162 GDPR defines statistical purposes as "any operation of collection and the processing of personal data necessary for statistical surveys or for the production of statistical results." The meaning of statistical purposes can be interpreted broadly and does not only cover uses for public interest, but may also include private entities doing research in pursuit for commercial gain.[91] Recital 162 GDPR also states, "The statistical purpose implies that the result of processing is not personal data, but aggregated data and that this result or the personal data are not used in support of measures or decisions regarding any particular natural person." It resembles Recital 29 DPD and it can be clearly followed that statistical analysis used for decision-making that directly affect a particular individual is not covered by the privileging rule.[92]

The use of personal data for scientific research—another privileged purpose—may also be interpreted broadly. Recital 159 GDPR mentions, for example, technological development and demonstration, fundamental research, applied research and also privately funded research. Studies conducted in the public interest in the area of public health are also explicitly referred to in the same recital as scientific research purposes.

The Regulation now refers in Article 5 (1) (b) to Article 89 (1). This article provides that processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall be subject to appropriate safeguards to protect the rights and freedoms of the data subject. Determining those

[89]Article 29 WP, p. 25; The Article 29 Working Party had investigated a considerable number of examples for further processing which is compatible and non-compatible. See Article 29 WP, pp. 51–69.

[90]Dix (2016), pp. 60–61; Sarunski (2016), p. 427; Boehme-Neßler (2016), p. 422; Bretthauer (2016), p. 271.

[91]Mayer-Schönberger and Padova (2016), p. 326.

[92]Mayer-Schönberger and Padova (2016), p. 327.

safeguards will be left to the Member States.[93] Article 89 (1) GDPR imposes some statutory requirements relating to the quality and conditions of the safeguards, which were not explicitly mentioned in the legal text of the Directive. For example, it is provided that the safeguards shall ensure the presence of technical and organizational measures in order to respect the principle of data minimization, for example, pseudonymization or anonymization subject to the circumstance that the purpose pursued with the processing can be fulfilled. In principle, it can be said, that Article 89 (1) GDPR reflects the approach previously suggested, and comprehensively set out, by the Article 29 Working Party in its Opinion on purpose limitation. There it is, inter alia, stated that different scenarios require different safeguards. There are scenarios where anonymized or aggregated data can be used; others require the processing of indirectly identifiable data or directly identifiable data.[94]

5.6 *The Waiver of the Requirement of a Legal Basis for the Processing of Personal Data that Qualifies as a Compatible Use*

The Regulation brought another change in respect of the purpose limitation principle that should not be overlooked. Recital 50 GDPR states that if the processing is compatible with the purposes for which personal data were initially collected, no legal basis separate from that which allowed the collection of the personal data is required. This is, at first glance, a surprising shift from the general rule that processing of personal data is prohibited unless covered by existing permissions. The questions arise, however, whether this change in the law is associated with considerable disadvantages for the data subject, and whether it significantly facilitates processing activities on the side of the data controller. Taking a closer look at the new provision on the compatibility assessment in Article 6 (4) of the Regulation, it appears that the interests of the data controller to further process the data and interests of the data subject shall be balanced. The same concept usually applies to a legal ground allowing the processing of personal data where the legitimate interests of the data subjects and data controller concerned are weighed against each other. This is, for example, especially reflected in Article 6 (1) (e) GDPR, which provides that processing of personal data shall be lawful if processing is necessary for the purposes of the legitimate interest of the controller or of a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data. Eventually, all legal grounds to be found in Article 6 (1)—and this applies also to the legal grounds established in Article 9 (2) GDPR—are the product of such a weighing of interests of the concerned parties—data subject and data controller—by the European legislator.

[93]Mayer-Schönberger and Padova (2016), p. 327.

[94]Article 29 WP, pp. 27–33.

Article 9 (2) of the Regulation, which concerns special categories of personal data, such as health data or genetic data,[95] provides specific legal grounds for processing such personal data. Due to the sensitive nature of the data and the increased demand for protection on side of the data subject, these legal grounds are generally stricter than those in Article 6 (1) GDPR: for example, consent must be explicit,[96] and a provision comparable to Article 6 (1) (e) GDPR allowing the processing of personal data if it is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data is not existent. One could argue that this specific protection mechanism established by Article 9 GDPR for special categories of personal data may be at risk to become undermined by the omission of the requirement of a legal ground for further processing of personal data that qualifies as a compatible use. However, Article 6 (4) GDPR should be flexible enough to take into account the degree of sensitivity of the data concerned, and to weigh them accordingly. Here the catalogue explicitly mentions that the nature of the data needs to be considered, as well as the possible consequences for the data subject. In order to protect the interests of the data subjects, data controllers that envisage further processing need to make the compatibility assessment in a careful and conscientious way and most probably will have to establish appropriate safeguards to protect the personal data at issue. Nevertheless, one cannot deny that there is a danger of misuse by the data controller through overemphasizing their own interests. In case of further processing for scientific purposes or statistical purposes, it is also interesting to consider that Article 9 (2) (h) GDPR largely resembles the requirements in Article 6 (1) (b) in conjunction with Article 89 (1) GDPR. This, in turn, points toward the conclusion that the data subject is neither placed in a less favorable position in the case of further processing of their personal data for statistical purposes, when the requirements of the privileging rule are fulfilled.

[95]Article 9 (1) Regulation (EU) 2016/679 defines special categories of personal data as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

[96]Article 9 (2) (a) Regulation (EU) 2016/679. For personal data that do not qualify as special categories of personal data in the sense of Article 9 (1) Regulation (EU) 2016/679, Article 6 (1) (a) Regulation (EU) 2016/679 states that processing of such data shall be lawful if the data subject has given consent to the processing of his or her personal data for one or more specific purposes. The standard for explicit consent remains the same as under the Data Protection Directive with the result that, for example, implied consent interpreted out of the data subject's conduct is not enough for an explicit consent in the sense of Article 9 (2) (a) Regulation (EU) 2016/679, but may be a sufficient legal basis for the processing of non-sensitive personal data in the sense of Article 6 Regulation (EU) 2016/679 (see Maldoff 2016).

6 Consequences of the Enactment of the GDPR for Big Data Applications and Conclusion

The Regulation retains the purpose limitation principle as one of its basic elements. Consequently, data controllers will, in the future, have to specify the purpose of the collection, which must be clearly and specifically identified. At the same time, in some fields, such as that of scientific and medical research, the European legislator has reacted on the issue of the necessity to reuse personal data and the difficulties to specify all research questions at the time of the collection of the data. Data subjects will be able to give their consent to certain areas of scientific research if ethical standards are complied with.[97]

Further processing of personal data under the Regulation will also need to be compatible with the original purpose for which the data was collected. The requirements regarding the permissibility of a change of purpose have not been loosened. Change of the purpose either needs to be covered by the privileging rule in Article 5 (1) (b) GDPR or pass the compatibility test, which is now explicitly incorporated into the legal text of the Regulation, namely Article 6 (4) GDPR. Further processing of personal data for scientific or statistical purposes shall be deemed in compliance with the purpose limitation principle, subject to appropriate safeguards. The latter, which should exclude or considerably reduce the risk for data subjects, remain (as was the case under the DPD) a matter to be implemented by Member States. A further limitation in such cases is that the processing at issue —including in Big Data scenarios—should not aim to gain information about particular individuals and/or make decisions affecting them. If it is otherwise, the principle of purpose limitation will again apply in full ambit, and the data controller will need to ask for the data subject's consent.

The legal situation under the new GDPR remains somewhat similar to the DPD with regard to the principle that personal data should not be kept in a form which permits identification of data subjects any longer than the purpose of the collection or reuse requires (Article 5 (1) (e) DPD). Again, though, personal data may be stored for longer periods insofar as they will be used solely for privileged purposes, such as statistical purposes or scientific research purposes (assuming appropriate technical and organizational measures to protect the data subject are in place).

Ultimately, then, it appears that the waiver of the requirement of a legal basis for further processing under the GDPR should not have a significant impact on the data subject's interests. These remain protected by the need in such circumstances for the data controller to satisfy the provisions of Article 6 (4), as well as those of Article 5 (1) (b) GDPR in conjunction with Article 89 (1) GDPR.

In short, the legal situation for data controllers wishing to process personal data in Big Data applications has—with regard to the purpose limitation principle—not significantly changed. It will remain a core issue how to specify the purpose of the

[97]Recital 33 Regulation (EU) 2016/679.

collection and further use of the personal data prior to, or at least no later than, the time of collection. As well as under the Directive the purpose specification requirement sets limits to open ended Big Data applications, where the purpose will only be specified after the analysis has commenced.

Big Data applications that involve further processing of personal data for scientific and statistical purposes do not face considerable obstacles if appropriate safeguards for the data subject are maintained. The establishment of such safeguards is, of course, consuming resources on the side of the data controllers. Data controllers wanting to further use personal data for Big Data analysis in order to gain information about particular individuals and/or make decisions affecting them do indeed face larger obstacles to further process the personal data in compliance with the purpose limitation principle. For example, if an organization is aiming to further process the personal data of their customers in order to analyze or predict the personal preferences and behavior of individual customers in order to use such information to base decisions regarding them, then the data controller will be required to obtain the informed consent of those customers.[98]

To conclude, it should also be pointed out that privacy, which the data protection regulations including the purpose limitation principle seek to realize, may not only be seen as a hindering factor for economy and science. European Network and Information Security Agency (ENISA), for example, recently noted that "if privacy principles are not respected, Big Data will fail to meet individual's needs; if privacy enforcement ignores the potentials of Big Data, individuals will not be adequately protected."[99] Involved stakeholders should work together in addressing the challenges and highlight privacy as a core value and a necessity of Big Data. Technology should be used as a support tool to achieve this aim.[100]

Acknowledgements This work has been supported by the EU project SoBigData (http://www.sobigdata.eu/) which receives funding from the European Union's Horizon 2020 research and innovation program under grant agreement No. 654024 and the German national project ABIDA (http://www.abida.de/) which has been funded by the Bundesminsterium für Bildung und Forschung (BMBF). The authors would like to thank Marc Stauch for his valuable support.

References

Albrecht JP (2016) The EU's new data protection law—how a directive evolved into a regulation. Comput Law Rev Int 17(2):33–43

Arbeitskreis Medizinischer Ethik-Kommissionen (2013) Mustertext zur Spende, Einlagerung und Nutzung von Biomaterialien sowie zur Erhebung, Verarbeitung und Nutzung von Daten in Biobanken. http://www.med.uni-freiburg.de/Forschung/VerantwortungForschung/mustertext-

[98]Article 29 WP, p. 46.

[99]European Union Agency for Network and Information Security (ENISA) (2005), pp. 17–18.

[100]European Union Agency for Network and Information Security (ENISA) (2005), pp. 17–18.

biobanken-deutsch.doc. Accessed 17 Nov 2016, English Version: http://www.ak-med-ethik-komm.de/index.php?lang=de. Accessed 17 Nov 2016
Article 29 Data Protection Working Party (2013) Opinion 03/2013 on purpose limitation, 00569/13/EN, WP 203
Beyleveld D (2004) An overview of directive 95/46/EC in relation to medical research. In: Beyleveld D et al (eds) The data protection directive and medical research across Europe. Ashgate Publishing Company, Burlington
Boehme-Neßler V (2016) Das Ende der Anonymität – Wie Big Data das Datenschutzrecht verändert. Datenschutz Datensich 40(7):419–423
Bretthauer S (2016) Compliance-by-design-anforderungen bei smart data. Z Datenschutz 6 (2):267–274
Bundeskartellamt, Autorité de la concurrence (2016) Competition law and data. http://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Big%20Data%20Papier.pdf;jsessionid=9F9A418331598CA75471DEA51872F638.1_cid371?__blob=publicationFile&v=2. Accessed 16 Sept 2016
Cavanillas JM, Curry E, Wahlster W (2015) The big data value opportunity. In: Cavanillas JM, Curry E, Wahlster W (eds) New horizons for a data-driven economy. Springer, Cham
Curry E (2015) The big data value chain: definitions, concepts, and theoretical approaches. In: Cavanillas JM, Curry E, Wahlster W (eds) New horizons for a data-driven economy. Springer, Cham
Dix A (2016) Datenschutz im Zeitalter von Big Data. Wie steht es um den Schutz der Privatsphäre. Stadtforsch Stat 29(1):59–64
European Union Agency for Network and Information Security (ENISA) (2005) Privacy by design in Big Data—an overview of privacy enhancing technologies in the era of Big Data analytics. https://webcache.googleusercontent.com/search?q=cache:bsgvi1hfgTYJ:https://www.enisa.europa.eu/publications/big-data-protection/at_download/fullReport+&cd=2&hl=de&ct=clnk&gl=de&client=firefox-b-ab. Accessed 4 Oct 2016
Ehmann E, Helfrich M (1999) Kurzkommentar zur EG-Datenschutzrichtlinie. Verlag Otto Schmidt, Cologne
Grützmacher M (2016) Dateneigentum – ein Flickenteppich. Comput Recht 32(8):485–495
Handelsblatt Research Institute (2014) Datenschutz und Big Data: Ein Leitfaden für Unternehmen. http://www.umweltdialog.de/de-wAssets/docs/2014-Dokumente-zu-Artikeln/leitfaden_unternehmen.pdf. Accessed 17 Nov 2016
Information Commissioner's Office (2014) Big Data and data protection. https://ico.org.uk/media/1541/big-data-and-data-protection.pdf. Accessed 28 Sept 2016
Kanellos M (2016) 152,000 Smart devices every minute in 2025: IDC outlines the future of smart things. http://www.forbes.com/sites/michaelkanellos/2016/03/03/152000-smart-devices-every-minute-in-2025-idc-outlines-the-future-of-smart-things/#4ec22cb069a7. Accessed 15 Aug 2016
Körber T (2016) "Ist Wissen Marktmacht?" Überlegungen zum Verhältnis von Datenschutz, "Datenmacht" und Kartellrecht – Teil 1. Neue Z Kartellr 4(7):303–310
Laney D (2001) 3D data management: controlling data volume, velocity, and variety. Technical report, META Group, https://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf. Accessed 16 Aug 2016
Maldoff G (2016) Top 10 operational impacts of the GDPR: Part 3—consent https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-3-consent/. Accessed 4 Oct 2016
Marnau N (2016) Anonymisierung, Pseudonymisierung und Transparenz für Big Data. Datenschutz Datensich 40(7):428–433
Martini M (2014) Big Data als Herausforderung für den Persönlichkeitsschutz und das Datenschutzrecht. http://www.uni-speyer.de/files/de/Lehrst%C3%BChle/Martini/PDF%20Dokumente/Typoskripte/BigData-TyposkriptiSd%C2%A738IVUrhG.pdf. Accessed 17 Nov 2016
Mayer-Schönberger V, Padova Y (2016) Regime change? Enabling big data through Europe's new data protection regulation. Columbia Sci Technol Law Rev 17:315–335
Medical Research Council (2011) MRC Policy and Guidance on Sharing of Research Data from Population and Patient Studies. http://www.mrc.ac.uk/publications/browse/mrc-policy-and-

guidance-on-sharing-of-research-data-from-population-and-patient-studies/. Accessed 29 Sept 2016
Metschke R, Wellbrock R (2002) Berliner Beauftragter für Datenschutz und Informationsfreiheit, Hessischer Datenschutzbeauftragter, Datenschutz in Wissenschaft und Forschung. https://datenschutz-berlin.de/attachments/47/Materialien28.pdf?1166527077. Accessed 28 Sept 2016
Raabe O, Wagner M (2016) Verantwortlicher Einsatz von Big Data. Datenschutz Datensich 40 (7):434–439
Roßnagel A et al (2016) Datenschutzrecht 2016 "Smart" genug für die Zukunft. Kassel University Press GmbH, Kassel
Sarunski M (2016) Big Data—Ende der Anonymität? Fragen aus Sicht der Datenschutzaufsichtsbehörde Mecklenburg-Vorpommern. Datenschutz Datensich 40(7):424–427
Schaar K (2016) DS-GVO: Geänderte Vorgaben für die Wissenschaft—Was sind die neuen Rahmenbedingungen und welche Fragen bleiben offen? Z Datenschutz 6(5):224–226
Turner V et al (2014) The digital universe of opportunities: rich data and the increasing value of the Internet of Things. Rep. from IDC EMC. https://www.emc.com/collateral/analyst-reports/idc-digital-universe-2014.pdf. Accessed 15 Aug 2016
Werkmeister C, Brandt E (2016) Datenschutzrechtliche Herausforderungen für Big Data. Comput Recht 32(4):233–238
Wolff H (2016) In: Wolff HA, Brink S (eds) Beck'scher Online Kommentar Datenschutzrecht, Prinzipien des Datenschutzrechts. https://beck-online.beck.de/Home. Accessed 17 Nov 2016
Zech H (2012) Information als Schutzgegenstand. Mohr Siebeck Verlag, Tübingen

Scientific Research and Academic e-Learning in Light of the EU's Legal Framework for Data Protection

Cecilia Magnusson Sjöberg

Abstract Scientific research and academic education are major, long-standing activities in our society. Digitalization has become a fundamental aspect of development and sustainability in these sectors and many others. New technologies and associated networks mean that the stage is now global. Internationalization is therefore a core characteristic of science. Adding to the picture is the fact that what emanates from the research community serves as basis for many other disciplines. Education based on scientific findings, not merely on opinions etc., is just one example hereof. This, in turn, requires an infrastructure that allows for digitalization with regard to research in itself, but also for learning purposes. The topic covers a wide area and will here be narrowed down to a study of current legal developments with regard to data protection for privacy purposes in the context of scientific research and academic e-learning, bearing academic freedom in mind. The analysis will be carried out in light of the EU's legal framework for data protection.

Keywords Research · e-Learning · Data protection · Privacy · Information security

Contents

C. Magnusson Sjöberg (✉)
Faculty of Law, Stockholm University, Stockholm, Sweden
e-mail: cecilia.magnussonsjoberg@juridicum.su.se

M. Corrales et al. (eds.), *New Technology, Big Data and the Law*,
Perspectives in Law, Business and Innovation, DOI 10.1007/978-981-10-5038-1_3

1 Introduction

1.1 Topic

This chapter will address two well-established activities in modern society, namely scientific research[1] and academic education.[2] The discourse focuses on *digitalization*, as both a contemporary enabler and a challenger of fundamental values in society, more specifically with regard to the sustainability of essential ideals. The development and use of Information and Communications Technologies (ICT) has a significant impact on these matters. Today, there is a *global* setting in which internationalization is a core characteristic of all kinds of research activities and study networks.[3] There are, of course, multifaceted ways for society to let science prosper both for its own good and with regard to needs within adjacent disciplines. Education based on scientific findings and not general views and opinions is just one example hereof. This, in turn, requires an infrastructure that allows for digitalization both with regard to research in itself and for the purpose of learning. The associated problem area is broad and will here be narrowed down to an investigation into current legal developments with regard to data protection for privacy purposes in the context of scientific research and academic e-learning, bearing academic freedom[4] in mind. The analysis will be carried out in the light of the EU's legal framework for data protection.

[1]When the term research is used in this text, it denotes scientific research and not other kinds of development, unless otherwise indicated.

[2]In addition to serving as a contribution to this publication, the text is a deliverable within the framework of the research project 'E-learning—A Legal Analysis Focusing on Employment Law, Copyright and Privacy protection' financed by the Marcus and Amalia Wallenberg Foundation, Sweden.

[3]See Jamin and van Caenegem (2016). See further Svantesson and Greenstein (2013) about internationalisation of law.

[4]See Carlson (2015) about Academic Freedom and the rights to university teaching materials pp. 356 et seq.

1.2 Focal Points

The current presentation allows for three major focal points. They are not to be viewed separately, although they are here introduced in that manner, for structural reasons. One central message is the imperative for *interplay* between scientific research, academic education, and ethical and legal compliance, all taking place in a digital environment.

A brief practically oriented illustration of this may be that of a computer linguist carrying out scientific research by means of data mining[5] in a so-called Big Data environment using a predictive modeling approach. An overall purpose could be that of developing privacy enhancing technologies that might, among other applications, be used in academic education teaching privacy by design. This in turn could be oriented towards a deepened understanding of privacy in the modern society. In addition, such an understanding could be a condition for compliance with regulations comprising ethical vetting as well as specific privacy safeguards. This all boils down to what may be referred to as Digital humanities, a label for a new research domain, which encompasses social sciences, linguistics and law. In this emerging interdisciplinary field, cultural changes of different kinds are investigated.[6]

The title of this chapter, "Scientific research and academic e-learning in light of the EU's legal framework for data protection," calls for an analysis directed towards certain core components, i.e., the focal points introduced so far.[7] In terms of hypotheses, scientific research appears to be prioritized in the General Data Protection Regulation (2016/679). At the same time, academic education seems to be burdened by the immense number of constraints with regard to data processing. Ethical and legal compliance is no doubt complicated, calling for a methodical approach in order to achieve fulfillment.

1.3 Chapter Structure

This chapter has the following structure. First, the topic at hand and associated focal points are introduced further. Given that the European Union serves as the regulatory platform for the analysis, the General Data Protection Regulation (GDPR) is presented, placing an emphasis on the conceptual basis related to core questions of

[5]See Colonna (2016) about Legal implications of data mining (2016). For a relatively early legal analysis of the rapidly emerging information society, see Lundblad (2007).

[6]In this context, an increasing interest for the interaction of law and media can be noted. See, for example, Lawyers in the media society (2016) and Society trapped in the network (2016). For a critical approach to science, technology and the future of humanity, see Häggström (2016).

[7]See Magnusson Sjöberg and Wolk (2012) for an introduction to E-learning from a legal point of view.

interpretation and application. This is followed by a more in-depth analysis of the focal points addressing how, from a regulatory point of view, scientific research is prioritized while academic education is burdened and the surrounding ethical framework is becoming increasingly complicated. Considering the author's national background, it appears worthwhile to include a brief outlook on the current Swedish approach to the problem area, followed by some concluding remarks.

2 EU General Data Protection Regulation

2.1 Presentation

Currently, until 25 May 2018, the EU Data Protection Directive (95/46/EC) is in force.[8] From that date there will, as already pointed out, be a different legal regime based on the completely new General Data Protection Regulation (GDPR).[9] The overall purposes of this data protection reform may briefly be summarized in terms of an intention to strengthen privacy, increase harmonization among member states, reduce bureaucratization, and accomplish better technical adjustments; all in all to strengthen the digital single market.

Of particular note is the shift from a EU directive to a regulation. This is clearly a way to stress the importance of data protection, as a regulation is applied directly in the member states, whereas a directive must first be implemented into national legislation. In practice, it can be expected that there will be more focus on the actual wording of the legal act emanating from the EU than before. Already in early preparatory studies different official language versions of the GDPR are studied by legal professionals and others.

Yet another issue to reflect upon concerns the impact of cases decided by the Court of Justice of the European Union (CJEU) or by national courts. After May 2018, the extent to which previous judgments will still—if at all—reflect what is deemed to be valid law will depend on quite a few different circumstances. Some

[8]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.

[9]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. This comprehensive data protection reform was initiated by the EU Commission presenting a first complete official draft 25.1.2012 COM(2012) 11 final. In addition to the GDPR, this has resulted in 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. The handling of passenger name records has also caused amendments in the data protection framework. The legal doctrine is catching up with the problem area. See, e.g., Blume (2016).

decisions will obviously no longer be relevant, while others indeed will be. One brief example of the latter is the ruling in the Google Spain case (C-131/12) concerning a data subject's right under certain circumstances to be "forgotten" by online search engines and the duties of removal on behalf of service providers. The right of erasure is explicitly regulated in Article 17 in the GDPR.

From a practical point of view, it is quite striking how complicated the new regulation has turned out, at least linguistically and structurally. There are 173 recitals and 99 articles, which could be considered to challenge readability (although not all provisions are applicable in every situation). The great number of abbreviations is also striking.[10] Given the current legal cultures, it is not surprising that the market for legal advice by way of for instance offering digital tools for data protection analyses and compliance support seems to be growing. This may also partly be explained by the new required *proactive measures* of data protection. For instance, Article 25 outlines data protection by design and by default. Article 35 sets out when there must be a data protection impact assessment, etc.

The comprehensive legal framework for personal data protection presented above mirrors the forthcoming governing regulatory environment for both scientific research and academic e-learning. No doubt there will be an effort among responsible parties to adhere to information duties; security measures, not least, to avoid high administrative fines. From the point of view of scientific research and academic e-learning it will be necessary to find a legitimate path in order to continue already on-going as well as forthcoming activities. A conceptual basis for realizing such an aim will be presented below.

2.2 The Swedish Regulatory Approach

In brief, the Swedish lawmaker has approached the EU data protection reform within the already existing framework for legislative matters. More precisely, this has entailed the appointment of a total of three generally oriented parliamentary inquiries aiming at (a) accomplishing a national supplementary regulation to the General Data Protection Regulation (EU 2016/679), (b) implementation into national law of the Directive on Data Protection in law enforcement (EU 2016/680), and (c) implementation into national law of the Directive (EU 2016/681) on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.[11]

[10]Examples of a few commonly used abbreviations include DPA (Data Protection Authority), DPO (Data Protection Officer) and DPIA (Data Protection Impact Assessment).

[11]Formal references to these governmental assignments are the following: Dataskyddsförordningen, Genomförande av EUs direktiv om skydd av personuppgifter vid brottsbekämpning, brottmålshantering och straffverkställighet, and, Genomförande av direktiv om användning av passageraruppgiftssamlingar.

In short, this legislative procedure consists of a parliamentary inquiry to investigate the assigned questions and present its conclusions in a public report, possibly including topic-oriented legislative proposals. The next step is for the relevant governmental ministry to distribute the proposals for public referral. Thereafter, the government might draw up a bill to be presented to the parliament for a decision whether it should be accepted or not. Depending on the topic at hand, the government might as a constitutional alternative be authorized to make a decision about a legislative act in the form of an ordinance instead of an act of law.[12]

The GDPR and how it is handled among the Member States is of primary interest for scientific research and academic e-learning. The Swedish regulatory approach is thus one of many. In this context, it is important to note that, in spite of the formal constraints of an EU regulation regarding the national scope of adjustments, the GDPR opens for both mandatory *and* optional national alterations. In Sweden, this has resulted in approximately twenty supplementary sector-specific inquiries, investigating the needs for GDPR assessments within for instance social insurance, work life, education and, last but not least, research.[13]

Historically speaking, it is unique to have so many legislative initiatives running simultaneously. Most must be completed by the spring/summer 2017 in order to be in force by 25 May, when the GDPR will be applicable. Most probably one of many results will be a specific Swedish law dedicated to privacy in connection with personal data processing for research purposes. Adding to the Swedish picture are the approximately 200 pre-existing laws and ordinances regulating personal data processing, primarily in the public sector.

In this context, it is important to note that, to the extent there is applicable member state law to which the controller is subject, such rules must be *proportionate* to the legitimate aim pursued. It also follows from Article 6 (3) last sentence that the lawfulness of processing requires that such law shall meet an objective of public interest.

2.3 Conceptual Basis

While this chapter is not a jurisprudential study, it cannot be disregarded that various terms and concepts have a substantive impact on interpretation and application of data protection law (in a broad sense). Having said that, the methodology here will be to narrow down the scope of analysis to a conceptual basis for scientific research and academic e-learning.

[12]See further Public Access to Information and Secrecy Act: Information concerning public access to information and secrecy legislation, etc. Swedish Government (2009) and The Constitution of Sweden: The Fundamental Laws and The Riksdag Act Revised. Swedish Parliament (2016). See also Magnusson Sjöberg (2007).

[13]See further instructions to the Research Data Inquiry, of which the author is the chair, Data processing for research purposes.

Bearing in mind that there is a whole family of concepts including for instance, research, researcher, research person, research body, etc., the focus will here be on scientific research from the perspective of data protection, and more precisely the GDPR. At the same time, the notion of academic e learning serves as a specific area of interest in itself, albeit also based on research activities and associated results in a broad sense. In this discourse, e-learning in academic environments, i.e., primarily higher education at universities, is considered in general terms, bringing to the fore digitalized teaching, associated electronic communication and documentation. This is similar to saying that the scientific research of today and associated academic e-learning activities call for *privacy awareness*. This is true not least considering technological developments with a whole set of emerging applications based on predictive modeling, blockchain technologies, artificial intelligence, etc.

Before moving on to the selected core questions of interpretation and application, a few observations will be made to well-established definitions closely related to research in a positive sense, for instance the concept referred to as *good research practice*. The Swedish Research Council's expert group on ethics[14] has highlighted the importance of researchers performing their work not only in an ethically well-considered manner, but also in compliance with applicable rules, regulations and guidelines. The approach in their report is practically oriented and broad, comprising any field of research, in an attempt to attract attention, in particular from postgraduates and their supervisors.[15]

In this context, mention should be made to the OECD definition of research and experimental development (R&D):

> Research and experimental development (R&D) comprise creative and systematic work undertaken in order to increase the stock of knowledge—including knowledge of humankind, culture and society—and to devise new applications of available knowledge.[16]

This general definition is further specified in a categorization of Basic research, Applied research and Experimental research:

> *Basic research* is experimental or theoretical work undertaken primarily to acquire new knowledge of the underlying foundations of phenomena and observable facts, without any particular application or use in view. *Applied research* is original investigation undertaken in order to acquire new knowledge. It is, however, directed primarily towards a specific, practical aim or objective. *Experimental development* is systematic work, drawing on knowledge gained from research and practical experience and producing additional knowledge, which is directed to producing new products or processes or to improving existing products or processes.[17]

[14]Of which the author currently is a member.

[15]See the Swedish Research Council's report on Good Research Practice 3_2011a. See further Magnusson Sjöberg (2005, 2016), Saarenpaa and Wiatrowski (2016), Saarenpaa and Sztobryn (2016), Strategier for Humanvetenskapliga området (2016–2018).

[16]OECD Frascati Manual (2015), p. 44.

[17]OECD Frascati Manual (2015), p. 45.

A way of describing what is referred to as *research integrity* is outlined by Science Europe, which is an association of European Research Funding Organizations (RFO) and Research Performing Organizations (RPO):

1. Research Integrity Safeguards the Foundations of Science and Scholarship;
2. Research Integrity Maintains Public Confidence in Researchers and Research Evidence;
3. Research Integrity Underpins Continued Public Investment in Research;
4. Research Integrity Protects the Reputation and Careers of Researchers;
5. Research Integrity Prevents Adverse Impact on Patients and the Public;
6. Research Integrity Promotes Economic Advancement;
7. Research Integrity Prevents Avoidable Waste of Resources.[18]

This text will not provide an in-depth analysis of the notion of research, in part because of the theoretical complexity as such, but also with consideration of how new information and communications technologies call for reshaping of research paradigms. Instead of, as is the convention, drawing up hypotheses beforehand, to be verified or falsified given certain legal developments, today's ICT opens the possibility for research where the central research issues are not necessarily defined beforehand. This is true not least within the legal domain where nowadays, for instance, probabilistic statistics are used for analyzing large volumes of decided court cases, automatic decision-making by public agencies, legally relevant behavior in social media, etc. Of course, digital environments such as Big Data, allowing for data mining, are particularly attractive in many research areas. This development is striking in legal research, where it historically used to be a major achievement on the part a legal scholar merely to find and retrieve legal information, commonly in the form of paper documents.

From the above follows a need for a good enough method with regard to a discussion about scientific research and academic freedom in light of the EU's legal framework for data protection. Therefore, the broad description of research in Recital 159 of the GDPR will have to suffice here:

> Where personal data are processed for scientific research purposes, this Regulation should also apply to that processing. For the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research. In addition, it should take into account the Union's objective under Article 179 (1) TFEU of achieving a European Research Area. Scientific research purposes should also include studies conducted in the public interest in the area of public health. To meet the specificities of processing personal data for scientific research purposes, specific conditions should apply in particular as regards the publication or otherwise disclosure of personal data in the context of scientific research purposes. If the result of scientific research in particular in the health context gives reason for further measures in the interest of the data subject, the general rules of this Regulation should apply in view of those measures.

[18]See further www.scienceeurope.org.

The above quoted Recital 159 and its general guidance for how to delimit scientific research is one of a cluster of recitals relevant to the research domain, including Recitals 160–162. Recital 156 lists guidelines for safeguards of a technical and organizational kind and specifications and derogations under particular conditions with regard to some of the data subject's rights, for instance information requirements, the right to be forgotten and data portability. In Recital 157, the advantages of joint processing of data from different files in registers are brought forward:

> By coupling information from registries, researchers can obtain new knowledge of great value with regard to widespread medical conditions such as cardiovascular disease, cancer and depression. On the basis of registries, research results can be enhanced, as they draw on a larger population. Within social science, research on the basis of registries enables researchers to obtain essential knowledge about the long-term correlation of a number of social conditions such as unemployment and education with other life conditions. Research results obtained through registries provide solid, high-quality knowledge which can provide the basis for the formulation and implementation of knowledge-based policy, improve the quality of life for a number of people and improve the efficiency of social services. In order to facilitate scientific research, personal data can be processed for scientific research purposes, subject to appropriate conditions and safeguards set out in Union or Member State law.

To summarize, the vocabularies surrounding research of different kinds are comprehensive and complicated. In this context, this has been illustrated by a few observations on what, in the broad community of research, is conceived of as good research practice, research integrity as well as R&D. Given the perspective of EU law applied here and, in particular, the GDPR, emphasis is placed on how the forthcoming regulation intends to master the balance of privacy protection on the one hand and society's quest for research on the other. A set of recitals has been the primary source for these reflections.

3 Core Questions of Interpretation and Application

3.1 Points of Departure

In this section, core questions of interpretation and application will be addressed in the perspective of the GDPR implying prioritized scientific research, burdened academic education and complicated ethical framework. The intention is not, in any way, to give a complete picture of the present situation, but rather to illuminate a set of critical factors reflecting current legal developments.

A fundamental concern has to do with the regulatory approach as such when the setting is digitalization in a global network society. Traditionally the lawmaker has aimed for technologically neutral legislation. In practice, this can be easier said than done. Modern information and communications technologies challenge fundamental legal infrastructures, in particular with regard to conventional manual data processing becoming automated, paper-based documentation being replaced by

electronic records and communication taking place beyond physical presence, in digital networks commonly associated with the Internet.

In response to this development, the future governing EU legal framework for data protection gives rise to a number of questions for interpretation and application with regard to new technology enabling for instance massive amounts of (personal) data to be collected, produced, modeled, processed, analyzed and managed for all kinds of purposes. The role of law in such a context must be *proactive* and not just reactive in order to have any kind of effect. Adding a legal perspective when privacy infringements have already taken place is not satisfactory.

3.2 Prioritised Scientific Research

This section will illustrate how scientific research is prioritized in the GDPR in comparison to other targeted processing purposes. A starting point is to recognize the notion of research and, more specifically, scientific research. Yet another term to be aware of is personal data processing for (scientific) research purposes. However, the GDPR does not make a distinction between research as such and research purposes.

A consequence of this is that, from a scientific point of view, it becomes more important to allow for a quite broad understanding of research. An example of this is the Swedish research project titled LifeGene[19] and how the Swedish government found it necessary to have the parliament enact a special law for consent-based processing of sensitive personal data for the purpose of future research.[20] A principal issue at stake here is whether the applicable legal framework allows for the development of *database infrastructures for scientific research purposes*. The underlying reasoning here is that it truly is an advantage, legally speaking, to have certain personal data processing formally labeled as scientific research. Some further points concerning the impact of these partly terminological aspects with regard to legitimacy and fewer duties etc., have been made above.

A second step in this overview is to pinpoint certain articles and recitals in the GDPR in order to establish, in particular, the lawfulness of processing (Article 6) and compliance with the general principles relating to processing of personal data (Article 5). Without going into any details, it can be concluded that there are

[19]See further www.lifegene.se and http://ki.se/en/about/lifegene-a-national-study-of-global-significance: "Karolinska Institute's LifeGene study is a national collaboration project designed to build a resource for research in all medical disciplines, facilitating new, ground-breaking research into the links between genes, environment and lifestyle. The study is an internationally unique initiative incorporating half a million Swedes that will create new tools for the prevention, diagnosis and treatment of the most common diseases."

[20]Lagen (2013:794) om vissa register för forskning om vad arv och miljö betyder för människors hälsa [English: Act (2013:794) on certain research registers regarding the impact of heritage and environment on people's health].

different legal conditions depending on the legal character of the responsible research body (in practice commonly the controller, see further the legal definitions in Article 4). A public authority is, for instance, unable to base its lawfulness of processing on a weighing of legitimate interests between a controller or third party, on the one hand, and the interests or fundamental rights and freedoms of the data subject which require protection of personal data (Article 6 (1) (f)), on the other hand. Instead, the lawfulness of personal data processing for research purposes will most probably be categorized as necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (Article 6 (1) (e)).

As regards consent there are both constraints and openings. A quite common approach to personal data processing for research purposes is to make it legitimate by way of the data subject's consent. As a rule, this will also be possible when the GDPR is applied in the future. Consent is now defined in Article 4 (11) in the following way:

> 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

This is all well and good as a starting point, but considering Recital 43 things get more complicated. This is because the requirement of consent being given voluntarily is somewhat strengthened in comparison to the Data Protection Directive (95/46/EC). A consequence of this is that the scope for lawfulness by way of consent is narrowed down when the research body (controller) is a public authority. This means that private research bodies, to a certain extent, have more alternatives with regard to accomplishing lawful processing:

> **Recital 43: Balanced consent**
>
> In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.

In spite of this limitation, Recital 33 opens for a relatively broader consent as regards the requirement of purpose specification in the context of scientific research:

> **Recital 33: Broad consent**
>
> It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognized ethical standards for scientific research. Data subjects should have the opportunity to give

their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose.

A project like the abovementioned LifeGene, which can roughly be described as the creation of a *database infrastructure* for research purposes, would seem to fall into the kind of specially treated category of research described above.

So far, the discussion has brought forward the vagueness and ambiguity of the terms research, scientific research and research purpose. Certain aspects of making personal data processing lawful by means of a weighing of interests, and making consent narrow and broad have also been observed. Now, the focus will shift to what may be referred to as the *research exemption* of the principle of purpose limitation as a fundamental principle of data protection. The starting point is Article 5 (b), which lays down the principle of "purpose limitation," including the abovementioned special rule applicable to scientific research etc.:

Personal data…

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89 (1), not be considered to be incompatible with the initial purposes ('purpose limitation');

The underlying reason for this exemption in the form of an exception is further commented on in Recital 50, which is also quoted here in spite of its quite lengthy wording, as it provides important context:

Recital 50: Research exception from the principle of purpose limitation

The processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected. In such a case, no legal basis separate from that, which allowed the collection of the personal data, is required. If the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Union or Member State law may determine and specify the tasks and purposes for which the further processing should be regarded as compatible and lawful. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations. The legal basis provided by Union or Member State law for the processing of personal data may also provide a legal basis for further processing. In order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, should take into account, inter alia: any link between those purposes and the purposes of the intended further processing; the context in which the personal data have been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their further use; the nature of the personal data; the consequences of the intended further processing for data subjects; and the existence of appropriate safeguards in both the original and intended further processing operations.

From the above, it follows, in short, that scientific research is not bound by the principle of purpose limitation when further processing personal data, as this is generally considered to be compatible lawful processing. While personal data

processing for research purposes is legitimate, fulfilling the general principles in Article 5 and the requirements of lawfulness of processing in Article 6, there are many further provisions to comply with. One example hereof is Article 9 regulating processing of special categories of personal data, i.e., sensitive data. Interestingly, this part of the GDPR contains another sign of how scientific research is being prioritized in the forthcoming regulation. More specifically, this follows explicitly from Article 9 (2) (j), which provides an exception to the general prohibition of processing for the listed special categories of personal data. Processing of special categories of personal data is with reference to Article 9 (2) (j) permitted if:

> (j) Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89 (1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

One of the most important provisions in the GDPR is probably Article 89 (1), regulating safeguards. No matter what other rules are followed by a controller and/or processor (see definitions in Article 4), consideration must always be made to these requirements when processing personal data for the purpose of, inter alia, scientific research.

> **Article 89 (1): Safeguards**
>
> Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes
>
> 1. Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organizational measures are in place in particular in order to ensure respect for the principle of data minimization. Those measures may include pseudonymization provided that those purposes can be fulfilled in that manner. Where further processing can fulfill those purposes, which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

It is of note, when applying this Article, that the requirements are not merely directed towards *safeguards* as such, but towards *appropriate* ones. Furthermore, there are two kinds of safeguards explicitly mentioned, namely technical and organizational measures. In this context, the principle of data minimization is brought forward, exemplified by *pseudonymization*. Even better, from the point of view of the rights and freedoms of the data subject, is of course processing that is completely *anonymized*, i.e., when data is no longer personal data according to the GDPR and thus falls outside the material scope (Article 2).

One current issue of interpretation and application concerns the potential of supplementary safeguards that may be referred to as legal ones. To exemplify what a legal safeguard might be, mention can be made of different kinds of regulations of secrecy and confidentiality, contractual clauses in addition to compulsory agreements between, e.g., a controller and processor, ethical vetting, etc.

Before continuing the discussion with some notes about "Burdened academic education," it is once more relevant to point at the technological challenges of accomplishing the kind of appropriate safeguards that the GDPR requires. Terms such as pseudonymization might at a first reading appear rather self-explanatory. This view is further strengthened by the seemingly clear-cut definition in Article 4 (5) of pseudonymization in the following way:

> 'pseudonymization' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

A more in-depth analysis shows that the complexity of pseudonymization as a data protection safeguard is much wider than what at least a legal expert might immediately realize.[21] This results in a need for legal experts to work together with technical experts throughout the development of digital architectures of various kinds. In such work, it is worthwhile to remember that everything that can be done in terms of personal data processing—including for the purpose of scientific research—does not necessarily have to be done. To refrain from adding new search criteria as a basis for joint processing of data from different files might be the best data protection safeguard of all.

3.3 *Burdened Academic Education*

The heading of this section is quite dystopian in its wording. In this context, it denotes the numerous *legal constraints* which are already a fact and which will most certainly increase as a result of the GDPR being applicable from 25 May 2018 onward. Of course, privacy is an important right within education, as well as in other segments of society. Having said this, it makes sense to allow for a problem-oriented exercise from the point of view of a university or other higher educational institution that is obliged to comply with the GDPR (and possibly other supplementary national legislation). As stated above, academic e-learning in light of the EU's legal framework for data protection calls for attention both during actual teaching activities, associated documentation and communication. Awareness of governing legal rules, no matter how onerous, is better than ignorance. With this in mind, a few comments should be made regarding core components of the GDPR from an e-learning perspective, as a kind of simple legal checklist. To avoid creating an expectation of a more in-depth analysis than is actually presented, there will be no explicit references to articles and recitals in the following.

Firstly, it is not particularly difficult for university management—which might be either public or private—to understand the overall value of data protection as a

[21] See, e.g., Gholami (2016).

means for *privacy* with regard to staff, students and third parties in the surrounding society. In a broad sense, staff may consist of both administrators and researchers, while students could pursue studies at different levels within the educational system. All these individuals have a right to expect protection of their personal data. At the same time, processing of personal data in connection with, for instance, experimental digital studies monitoring individuals is another side of the coin that may, to a varying extent, be considered legitimate and thus in contrast with the need for data protection.

The scope of the EU's data protection regulation is indeed broad. A striking amount of data is legally defined as direct or indirect information associated with living persons. The understanding of what is deemed as processing of such personal data is also very broad, as it comprises almost anything that could be carried out using information and communications technologies. This means that a modern university is processing personal data throughout its different e-learning activities. Given this fact, all e-learning actions must take place within the scope of the GDPR.

There is a large number of legal definitions of different aspects of data protection that universities engaging in e-learning must deal with. In addition to the already existing organization of administration, etc., the university must acknowledge its role as controller and possibly also processor, as well as appointing a data protection officer, etc. Although *privacy by management* is not a formally established term, it reflects the need for foreseeability in dealing with all kinds of data protection issues connected to e-learning. Of particular relevance in this context is whether the back-office is centralized or decentralized, authorizing different departments to be in control of ICT support, in spite of the overall responsibility falling on the vice-chancellor. In other words: who is authorized to design, procure, implement and further develop e-learning applications for cross-border online courses and classes and what is this authorization based on?

The area of data protection is characterized by many different principles. There are major principles of lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, as well as accountability. At first sight, this enumeration gives the impression of a set of general values to strive for. However, this is a dangerous approach as data protection in practice, including decisions by both courts and supervisory authorities, shows that assessments of fulfillment of these kinds of *coded principles* can very well be decisive for what is deemed permitted or prohibited, respectively.

New rules on lawfulness of processing in the GDPR set a somewhat different stage for universities depending on whether they are public or private bodies. As explained above, public authorities can no longer find support for legitimate personal data processing as a result of weighing of interests between an individual data subject on the one hand and the controller (or third party) on the other. Presumably e-learning activities as such may be considered necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. This is not the same as saying that all e-learning activities can be regarded as lawful processing. Is it, for instance, quite clear that activity on social

media such as Facebook as part of an *e-learning syllabus* is to be categorized as being of public interest?

Consent has been discussed from a regulatory point of view above. This perspective raises issues regarding whether a public sector university is at all able to base its legitimacy of personal data processing on consent due to a clear imbalance between students and teachers. A private university is at least not from a formal point of view hindered from using consent as a way of achieving lawful processing. There is still a challenge though, as a valid consent presupposes a freely given, specific, informed and unambiguous indication of the data subject's wishes. However, considering that more or less all e-learning activities result in some form of exam, commonly in a digital format, the scope of consent is limited. It boils down to a risk of consent as a fiction rather than a realistic option.

Processing of so-called special categories of personal data and also data relating to criminal convictions and offences is probably not the first thing e-learning is associated with. Given what is considered sensitive data, it is difficult—if at all possible—to completely avoid data processing comprising this kind of information. Students, and employees too, are faced with these sensitive special categories of personal data not only as registered parties within an educational institution, but also when carrying out learning exercises of different kinds. One example is law students, who are regularly required to search for court cases that to a considerable extent comprise personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data (for the purpose of uniquely identifying a natural person), data concerning health or data concerning a natural person's sex life or sexual orientation. The GDPR allows for quite comprehensive exceptions to the major rule that prohibits processing of this kind of sensitive data. In an e-learning environment, it is important to be aware that general browsing on the Internet, for instance, is not equivalent to more targeted data collection and digital analyses. Expressed in another way, e-learning providers must consider the fact that different categories of personal data must be treated accordingly from a data protection point of view. Privacy-sensitive e-learning is to be regarded as a goal.

The rights of a data subject are strengthened by the GDPR. Briefly, this concerns information duties, rights of rectification, erasure ("the Right to be Forgotten"), data portability, rights to object and conditions for automatic individual decision-making, including profiling and much more. Meeting such requirements on a daily basis demands resources of different kinds. University staff must be educated and furthermore data protection rules must be integrated into other legal frameworks, for instance rights of access for the purpose of transparency, etc. In a university setting, this might be more of a challenge than in a conventional public authority or within a private company. This is at least partly explained by the fact that e-learning, as addressed here, takes place within academia. Academic freedom is fundamental among both researchers and students at undergraduate and postgraduate level, as well as those pursuing doctoral studies. To have such a diverse organization respond adequately to the kind of regulatory framework represented

by the GDPR is a test in its own. Legalizing e-learning in academia must be a top priority.

As already pointed out, the need for law to play a *proactive* role cannot be underestimated when striving for privacy. By formally requiring data protection by design and by default, the EU takes a clear step towards efficient law-making. This is necessary as a response to the digitalization of society of which education by way of e-learning is a very good example. It is for instance not particularly wise to design a learning management system without taking data protection into consideration at early stages of system development. Furthermore, the costs to rectify insufficient information security measures risking data integrity (correctness) and confidentiality (secrecy) can be very high, not least in terms of administrative fines. One method to prevent this at least partly is to carry out data protection impact assessments. This would also be valuable when e-learning takes place beyond a particular member state or in a so-called third country outside of the EU. Needless to say, as soon as you go digital in a modern Internet-related network, data will cross national borders,[22] which in turn will trigger the GDPR's strict rules on third country transfers. In reality, this will happen on a daily basis as students from different universities get in contact with each other online, both formally and informally, as a matter of course. To conclude, there is a need for a *holistic approach* when the educational environment becomes more and more international.

3.4 Complicated Ethical Framework

It has become increasingly common to explicitly address ethical and legal issues in projects including personal data processing for research purposes. Generally speaking, this comes quite naturally during the stages of initiating a project, seeking funding, finding partners from both the public and private sector with different national origins, etc. At early stages of project management, ethical and legal awareness is equally important as continuously paying attention to the interplay between *ethics and law* in the context of the research questions at hand.

In response to this, Recital 33 of the GDPR opens for what may be referred to as a broad *consent*, however conditioned with "when in keeping with recognized ethical standards for scientific research" (see above). Through this wording, the Regulation makes it necessary for the research body (controller/processor) to not only be aware of the existence of ethical standards as such, but also to assess whether they are acknowledged and, as a next step, to adhere to them. What seems to be missing are more precise evaluation criteria of what is to be understood as "recognized ethical standards." Presumably, this will be a task for law to clarify in practice.

In addition to ethics under certain circumstances being an important component when seeking a data subject's consent, it could arguably also serve as a safeguard in

[22]Regarding extraterritoriality see, e.g., Svantesson (2013).

itself (Article 89 (1)). While the Regulation does not explicitly bring in ethical vetting as a safeguard, it appears as if a national legally based system for ethical assessments could be conceived of as a legal safeguard within the GDPR framework. The Swedish Act (2003:460) on ethical vetting of research that involves humans[23] may serve as an example. In brief, this law requires an ethical review as soon as either sensitive personal data or data concerning violation of laws—as defined in the national implementation of the Data Protection Directive (95/46/EC)—are being processed for research purposes.[24]

At first glance, it might appear self-evident that ethics has an important role to play in data protection. However, the path forward is not clearly marked. Just to illustrate, it is not obvious how to decide the scope of an ethics review; how to define (scientific) research in this context, how to organize the vetting within primarily legal and national organizational infrastructures,[25] applicable fees, etc. Furthermore, if the substantive scope of a regime for ethics is implemented, is this similar to saying that, for instance, all processing of sensitive data formally speaking is to be included, no matter whether the data in question is already made officially available online in the form of decided court cases? Or is there reason to make a distinction between, for instance, structured information by using different kinds of database technologies allowing for mark-up on the one hand and unstructured text on the other? Then again, it cannot be ruled out that the risks of privacy infringements might be higher in a research environment where individual researchers deal with pieces of sensitive information in ordinary documents, rather than in controlled laboratories, where the general understanding of privacy-enhancing measures including risk assessments and management might be much higher.

In spite of the challenges associated with ethical vetting for the purpose of privacy in connection with personal data processing, the potential is large. It is a way of transforming the requirement of appropriate safeguards as per the GDPR (Article 89 (1)). It follows from the reasoning above that ethical vetting could qualify as a legal safeguard supplementing technical and organizational safeguards. It is, of course, not possible to draw up borders between these categories that are precise enough to serve as guidance for responsible parties.

[23]Lag (2003:460) om etikprövning av forskning som avser människor.

[24]According to Sect. 2 of the Ethics Review Act "research" is understood to mean not only scientific, experimental or theoretical work to obtain new knowledge, but also developmental work carried out on a scientific basis, with the exception of that which is carried out as part of a programme of study at an institute of higher education at a basic or advanced level. See further http://www.epn.se/en/start/. Accessed 10 Jan 2017. This legislation is currently investigated by a parliamentary inquiry, more precisely with regard to the boundary between clinical research and healthcare.

[25]A recent government report addressed the need for amendments of the Swedish organisation for ethical reviews of research.

4 Concluding Remarks

The initially introduced focal points have proved to be valid for a discussion about "Scientific research and academic e-learning in light of the EU's legal framework for data protection." Without any ambition of an exhaustive survey, certain concluding remarks can be made with regard to the forthcoming EU regulation of personal data processing. Firstly, scientific research appears to be given a relatively strong position in comparison with other sectors of society. In contrast, legal conditions for academic e-learning are surrounded by a large number of articles in the GDPR that are further illuminated in the recitals of the regulation. Adding to the picture is the fact that the interaction of ethics and law needs attention in itself, i.e., not merely as a support function to scientific research and academic education.

From the above it follows that the core hypotheses set out at the beginning have been verified. This is, of course, rewarding from a theoretical point of view. But what is the way forward? An attractive path is no doubt the emerging legal culture associated with *Digital humanities*, which in its modern approach intertwines long-since well-established scientific research areas. They comprise, in particular, social sciences, linguistics and law.

The legal perspective is quite naturally associated with the scientific research field of law and informatics.[26] More precisely, this research field has its basis in law with an interdisciplinary connection to computer science. This implies an interest for legal system management in terms of embedding law in the early stages of system design and/or procurement, implementation and further developments.[27] In addition to this methodological approach there are of course many substantive law issues associated with digitalization. Data protection, copyright, and e-government are just a few examples of areas that have for a long time and continuously called for legal attention. The need to let law play a proactive role and not merely act as a reactive tool when things have already gone wrong could be referred to as a scientific research paradigm in the Nordic countries.[28]

So what does the above analysis boil down to? Emphasis has been placed on Digital humanities as a way forward. In this context, the research field of Law & Informatics is relevant and promising as an enabling approach. One possible facilitator from a legislative point of view is increased focus on ethical safeguards possibly laid down in law. This is, however, not the same as saying that legislative measures are a success factor per se; in practice, they can turn out to be quite the opposite.

[26]The topic is presented by Magnusson Sjöberg (2016).

[27]For a presentation of the approach see Legal Management of Information systems: incorporating law in e-solutions (2005). A more recent contribution illuminating one of the core themes of legal automation is Schartum (2016), pp. 27 et seq.

[28]See, e.g., A Proactive Approach (2006), pp. 13 et seq.

What is sought for is rather a fusion of ethical standards in a legal context enhancing privacy by means of personal data protection. In terms of legislative techniques, technological neutrality remains valid given the rapid development of new technologies. From a legal point of view there will always be new means for information processing that are more or less possible to categorize within the legal domain. The label, as such, is commonly not decisive for a legal analysis. Data processing referred to as "Cloud computing" is topical with regard to legal consequences of outsourcing. Big Data and associated data mining are other applications of ICT implying a need for legal analyses of how data are made available for further handling. It should be noted that personal data processing is here understood broadly, with consequences not only for legal infrastructures, but also for technical and organizational ones.

What does matter is the possibility to provide lawyers with facts and explanations concerning what data are being processed, where, by whom and for what purpose(s). Only in doing so will it be possible to carry out scientific research and academic e-learning in clear light of the EU's legal framework for data protection.

References

Blume P (2016) Den nye persondataret: persondatafordningen (about the new personal data protection regulatory framework). Jurist og Ekonomforbundets Forlag, Copenhagen

Carlson L (2015–2016) Academic freedom and the rights to university teaching materials: a comparison of Swedish, American and German approaches. JT, Stockholm

Colonna L (2016) legal implications of data mining: assessing the European Union's data protection principles in light of the United States government's national intelligence data mining practices. Ragulka, Stockholm

Gholami A (2016) Security and privacy of sensitive data in cloud computing, doctoral thesis in high performance computing. KTH Royal Institute of Technology, School of Computer Science and Communication, Stockholm

Gustafsson B, Hermerén G, Pettersson B (2011) Swedish Research Council's report on good research practice 3:2011a translation based on report 1:2005 www.vr.se/download/18.3a36c20d133af0c1295800030/1340207445948/Good+Research+Practice+3.2011_webb.pdf . Accessed 17 Dec 2016

Häggström O (2016) Here be dragons: science, technology and the future of humanity. Oxford University Press, Oxford

Jamin C, van Caenegem W (2016) (eds) The internationalisation of legal education. Ius Comparatum—Global Studies in Comparative Law. Springer, Cham

Lundblad N (2007) Law in a noise society: ICT-policy making and societal models. Department of Applied Information Technology, University of Gothenburg http://noisesociety.com/t/manus200701106.pdf. Accessed 2 Jan 2017

Magnusson Sjöberg C (2005) (ed) Legal management of information systems: incorporating law in e-solutions. Studentlitteratur, Lund

Magnusson Sjöberg C (2006) Presentation of the Nordic school of proactive law. In: Wahlgren P (ed) Scandinavian studies in law, vol. 49, A Proactive Approach. Stockholm Institute for Scandinavian Law, Stockholm

Magnusson Sjöberg C (2007) Constitutional rights and new technologies in Sweden. In: Leenes R, Koops BJ, de Hert P (eds) Constitutional rights and new technologies: a comparative study, information technology and law series 15. TMC Asser Press, The Hague

Magnusson Sjöberg C, Wolk S (2012) Juridiken kring e-lärande (About law governing e-learning). Studentlitteratur, Lund

Magnusson Sjöberg C (2016) (ed) Rättsinformatik: Juridiken i det digitala informationssamhället, (About legal informatics: law in the digital information society). Studentlitteratur, Lund

OECD Frascati Manual 2015, Guidelines for Collecting and Reporting Data on Research and Experimental Development. www.oecd-ilibrary.org/docserver/download/9215001e.pdf?expires=1481958736&id=id&accname=guest&checksum=D1BF4BEFAA3E9501A6F2151FFE341253. Accessed 17 Dec 2016

Saarenpää A, Sztobryn K (2016) Lawyers in the media society: the legal challenges of the media society. University of Lapland, Rovaniemi

Saarenpää A, Wiatrowski A (eds) (2016) Society trapped in the network: does it have a future? University of Lapland, Rovaniemi

Schartum DW (2016) From algorithmic law to automation-friendly legislation. In: Bygrave L, Dobus E (eds) Science Europe, seven reasons to care about integrity in research, science Europe working group on research integrity—Task group "Knowledge Growth D/2015/13.324/2 www.scienceeurope.org. Accessed 28 Dec 2016

Svantesson DJ (2013) Extraterritoriality in data privacy law. Ex Tuto, Copenhagen

Svantesson DJ, Greenstein S (2013) (eds) The internationalisation of law in the digital information society. Ex Tuto, Copenhagen

Strategier för Humanvetenskapliga området, (2016–2018) Stockholms universitet (Eng. Strategies for Humanities)

The Constitution of Sweden: The Fundamental Laws and the Riksdag Act Revised. Swedish Parliament (2016)

Internet of Things: Right to Data from a European Perspective

Christine Storr and Pam Storr

Abstract The amount of data collected and processed by smart objects has increased exponentially over the last few years. The use of this technology, known as the Internet of Things or IoT, leads to new challenges and applications of existing data protection laws. Data resulting from the use of such technology has wide-ranging consequences for individual privacy as a large amount of the data in question is often personal in nature. However, the Internet of Things has a wider impact and also creates questions within such fields as contract law and intellectual property law, due in part to the lack of a clear property right to data. In addition, issues of data security are of importance when such technology is used, particularly when considering liability for data loss. This chapter will deal with the legal issues connected to the Internet of Things from a European perspective, taking into account existing laws and in light of the new European Data Protection Regulation. The underlying theme of the chapter focuses on the existence of legal rights to data created through the use of the Internet of Things and the various stakeholders that may have an interest in the data, from the service provider and the individual user, to intermediaries and those involved in allowing smart objects to fulfill their potential. The question of whether the legal challenges identified in the chapter can be overcome will also be addressed, along with the future role of law in the use and development of the Internet of Things.

Keywords Internet of Things · Right to data · Data protection · Security · Copyright

C. Storr (✉)
Faculty of Law, Stockholm University, Stockholm, Sweden
e-mail: christine.storr@juridicum.su.se

P. Storr
Legal Consultant and Teacher in IT law, Stockholm, Sweden

M. Corrales et al. (eds.), *New Technology, Big Data and the Law*,
Perspectives in Law, Business and Innovation, DOI 10.1007/978-981-10-5038-1_4

Contents

1 Introduction

Health devices such as fitness trackers and smart scales are growing in number, home appliances are becoming more connected, and smart city projects are popping up around the world. These smart devices and the environment surrounding them is referred to as the Internet of Things (IoT) . The IoT raises many questions from a legal perspective. Besides issues of liability where an IoT service, sensor or device does not function correctly,[1] the question of who owns the data that is being collected, analyzed and stored seems a rather important one.

There are many economic interests in data relating to the IoT, due to its value and potential for furthering industry development. The question that arises is whether these economic interests should be protected from a legal point of view, and if so, how. These interests may be held by a number of different stakeholders

[1]European Commission (2016), p. 22.

because of the way the IoT works in practice. The complexity of the question is also affected by the fact that data within the IoT often relates to specific individuals, and therefore constitutes personal data. A potential for conflicting interests in the same data is therefore created.

From a business perspective, personal data has a great value, being referred to as "the new oil of the Internet and the new currency of the digital world."[2] At the individual level, data subjects have a number of legitimate rights relating to their own data. It must therefore be decided which rights take precedence and how those involved in the provision of IoT solutions fulfill their legal duties towards the data subject and protect IoT data in practice.

To what extent the current legal framework provides for legal rights and duties in relation to data. Impact of the legal framework on the IoT solutions and stakeholders involved.

2 The Internet of Things (IoT)

The term "Internet of Things" is often attributed to Kevin Ashton.[3] In 2009, he mentioned the need for an Internet for Things as "a standardized way for computers to capture information from the real world and to understand it."[4] The IoT European Research Cluster (IERC)[5] defines the IoT as "a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual 'things' have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network."[6]

From a technical perspective, the IoT combines hardware (connected devices), software (IoT platforms) and services (IoT applications).[7] Devices can be dedicated IoT devices, sensors can be integrated into other devices or as software on existing devices. There can, therefore, be several platforms that store data collected through IoT devices and sensors.

Although the concept "Internet of Things" can be hard to define in a precise manner, an interesting analogy has been made describing the IoT as "extending the original concept of hyperlinking to include physical objects."[8] This linking of

[2]Kuneva (2009).

[3]Massachusetts Institute of Technology's Auto-ID (for Automatic Identification Center in Boston), at that time employee of Procter and Gamble.

[4]Ashton (2009), European Commission (2016), p. 5.

[5]The aim of the IERC is "to address the large potential for IoT-based capabilities in Europe and to coordinate the convergence of ongoing activities." See www.internet-of-things-research.eu/index.html. Accessed 10 Jan 2017.

[6]See www.internet-of-things-research.eu/about_iot.htm. Accessed 10 Jan 2017.

[7]European Commission (2016), p. 6.

[8]DuBravac (2014), p. 4.

physical and digital is at the heart of the IoT. It explains why terms such as "Industry 4.0"[9] and "smart" have been used, focusing on the nature of the things or objects involved. Smart cities, smart appliances, smart objects and smart cars are just a few examples of IoT applications. The environment has even been described as having a magical quality: a "world of 'enchanted objects,'…augmented and enhanced through the use of emerging technologies…so that it becomes extraordinary."[10]

2.1 IoT Statistics

The IoT is already being used today on a large scale, with the number of business-to-business connections surpassing 1 billion in 2014.[11] Estimates and projections of future IoT use differ, but there is a clear consensus that the number of IoT devices will increase dramatically over the next few years. Recent reports estimated that less than 1% of objects are currently connected to the Internet.[12] Gartner, for instance, predicts more than 10 billion "things" will be connected by 2018[13]; ABI Research estimates more than 30 billion devices by 2020[14]; Cisco's figures exceed both of these, predicting 37 billion by 2020.[15]

Even predictions in the area of home appliances and personal devices are high. Gartner predicts that by 2020, 20% of homes will contain at least 25 things accessing the Internet and 85% of home solutions will be linked to a certified ecosystem.[16] Further predictions include that in 2020, 477.75 million wearable electronic devices will be sold, generating revenue of $61.7 billion, of which $13.7 billion will be on fitness-related wearables.[17]

Potential future revenue from the IoT is staggering; McKinsey Global Institute estimates the potential annual economic impact to be $2.7 trillion to $6.2 trillion by 2025,[18] while Cisco estimates the IoT will create $14.4 trillion in value between 2013 and 2022.[19]

[9]Grützmacher (2016), p. 485.
[10]Rose (2014), p. 47.
[11]Verizon (2015), p. 4.
[12]IDC and TXT Solutions (2014).
[13]Gartner (2016b).
[14]ABI Research (2013).
[15]Cisco (2013), p. 2.
[16]Gartner (2016b).
[17]Gartner (2016a, b).
[18]Manyika et al. (2013), p. 12.
[19]Bradley et al. (2013), p. 1.

2.2 IoT and Big Data

Companies use collections of data for analysis already today. Currently, approximately one third of businesses use Big Data for strategic decisions.[20] As more IoT solutions are introduced, the number of data sets produced and analyzed will increase. Businesses will have access to previously unknown information, collected from IoT devices and sensors, which can then be used as a basis for decision-making. It is, therefore, likely that IoT data will increasingly be used as part of businesses' Big Data analytics, in turn impacting upon their strategic decision-making. As has been noted, "the value of Big Data is not in the mere data collection but in the insights deduced from it."[21]

2.3 IoT Scenarios

IoT technologies—partly already today—play a major role within the areas of smart homes, smart health, smart manufacturing and smart cities.[22] We will refer back to these four examples, detailed below, in order to illustrate legal issues in an IoT context.

Smart homes allow users to connect their home devices such as electricity, lights, heating, air-conditioning, blinds, fridges and coffee machines. A scenario that is already a reality today is that a user is about to enter her home and the geolocation on her mobile phone triggers the light on the porch, opens the lock on the front door, turns up the heating, opens the blinds and switches on the TV. In addition, with one button, the user has the ability to turn off *all* appliances when she leaves the house. Appliances may be able to be controlled remotely, for example, to turn the heating off when nobody is at home, or to turn it back on in preparation for someone arriving home. Smart homes may also include the possibility to automatically adapt the temperature according to the weather conditions that are measured by a sensor outside the house; the same sensors can also be used to automatically water plants if, for example, there has been a long period of sun.[23]

Smart health devices have already started emerging among a wide consumer population. Wearable fitness trackers can measure data such as steps taken, floors climbed, calories burned and hours of sleep. This data can then be used to help improve personal health, to control one's weight or as a basis for a fitness regime.[24] The trackers can either be used via the sensors on existing smart phones or as

[20]Ernst and Young (2015), p. 11.

[21]Custers and Uršič (2016), p. 7.

[22]European Commission (2016), p. 26.

[23]See, e.g., European Commission (2016), pp. 31–32.

[24]See, e.g., European Commission (2016), p. 33.

stand-alone wearable devices (often watches) that sync the data with a smart phone or are embedded in clothing, fabrics or other devices attached to the body.

Smart manufacturing aims at making factory automation more energy efficient with higher flexibility in production and lower operational costs. With the help of IoT sensors factory machines can be maintained quicker, thereby increasing the safety of the production process.[25] By including statistical and real-time customer data in the context of manufacturing, transport and warehouse costs can be decreased.

Smart cities allow more efficient planning of public transport (buses and trains can be sent to the places that house more people at a given time), more environmentally-friendly use of resources (e.g., street lights can be dimmed depending on the weather and light conditions), and more efficient waste and energy management. A smart city can combine different infrastructures of a modern city such as energy, buildings, water management, lighting, environment, public transport, waste management, traffic, etc., into one interconnected ecosystem.[26] More than 100 cities from 23 countries in Europe, Latin America and the Asia-Pacific region are already cooperating through the Open and Agile Smart Cities initiative.[27]

2.4 Stakeholders and Data in the IoT Ecosystem

There are often a number of different stakeholders involved in the IoT ecosystem. Some, or all, of the following may be needed for a particular IoT solution: device manufacturers, sensor manufacturers, software and application developers, infrastructure providers, and data analytics companies.[28]

In a smart home setting, for example, there are different stakeholders that provide the hardware, e.g., lights, heating, electronic appliances. Some of the hardware providers might offer the software and a service at the same time, e.g., Philips Hue smart lights include the light bulbs, a router, the connectivity between the devices and apps for different smart phones. In other cases, one provider will produce the hardware (e.g., a TV), another an additional device to make the TV IoT-friendly, and another an application that lets you control the appliance through the IoT device and set up home automation through a third-party web service.[29]

---

[25]See, e.g., European Commission (2016), pp. 33–34.

[26]European Commission (2016), p. 35.

[27]See www.oascities.org. Accessed 10 Jan 2017.

[28]European Commission (2016), p. 22.

[29]For example, you can use a Belkin Wemo Switch to make your lights at home IoT compatible. The switch is added in between the power plug and the lamp and provides IoT connectivity, which means you can access your lights remotely and switch them on and off through an app on your smart phone. In addition, you can use a service such as IFTTT (If This Then That) to connect the lamp with the geolocation of your smart phone, so the lights are automatically switched on when you approach your house. See www.belkin.com/us/Products/home-automation/c/wemo-home-automation/, http://www.philips.co.uk/c-m-li/hue-personal-wireless-lighting and https://ifttt.com/. Accessed 10 Jan 2017.

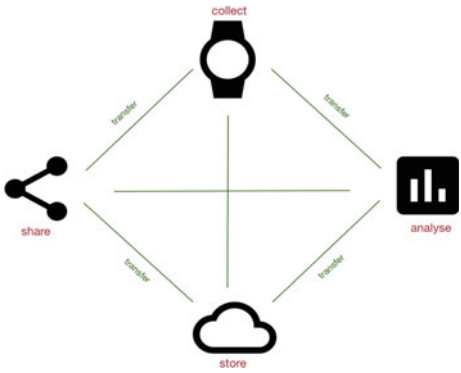

Fig. 1 Data processing ecosystem

The high number of potential stakeholders leads to increasing technical challenges and incentives to share data, as "sophisticated interdependencies between product and service producers" are created.[30] For the IoT ecosystem to work as intended it is often important, and perhaps even necessary, for data to be shared between the various stakeholders.

From a technical point of view, data processing occurs when any action is carried out on data; for example, when data is collected, stored, transferred or analyzed. Data that is collected via an IoT sensor or device may stay on that device, be transferred to the Cloud for storage, be transferred to an organization for analysis, or be shared within a local network or a third party. From a combined IoT and Big Data perspective, we will build our analysis on the following data processes[31] (Fig. 1):

2.5 IoT Development in the EU

The last few years have seen the EU focus specifically on the IoT ecosystem. Through various strategies and initiatives, the EU has highlighted the perceived importance of the IoT. It is part of the EU Commission's Digital Single Market (DSM) strategy, the completion of which is one of the Commission's ten political priorities.[32] Besides Big Data and Cloud services, the IoT is seen as "central to the EU's competitiveness."[33] It is estimated that the EU IoT market will account for more than €1 trillion by 2020.[34]

[30]European Commission (2016), p. 22.

[31]Data processing is in practice a lot more complex, as the processes may be more intertwined and multifaceted. The legal analysis will, however, not necessarily differ as it still assumes the same types of processing.

[32]European Commission (2016), p. 4.

[33]European Commission (2016), p. 14.

[34]IDC and TXT Solutions (2014).

The focus of the EU is threefold: a single market for the IoT (devices and services should be able to connect seamlessly anywhere in the EU); a thriving IoT ecosystem involving open platforms; and a human-centered IoT (values such as the protection of personal data and security should be highly regarded).[35] To encourage the development of IoT research and market innovations, the European Commission established the Alliance for the Internet of Things Innovation (AIOTI) in 2015.[36] The EU also initiated the IoT European Research Cluster (IERC), which coordinates EU-funded projects on IoT technologies.[37] In addition, a European data economy initiative was proposed in January 2017,[38] helping the creation of a European single market for the IoT and discussing, amongst other things, liability issues in an IoT environment.[39]

3 Right to Data: A Business Perspective

Due to the economic importance of data for businesses the question arises whether a business or any organization collecting, storing, analyzing and/or sharing data in the IoT environment has a right to the data it processes. Considering the lack of a clear-cut or clearly established right to data in EU legislation,[40] we will discuss several different potential options for businesses that might, at least in theory, indirectly stipulate such a right.

To show the potential consequence of any right to data, we can use the scenario of smart cities (see Sect. 2.3). A city public transport system may have multiple forms of transport—train, bus, metro, tram, etc. Let us assume that one company has developed an IoT solution for the bus and tram network, with another developing a solution for the train and metro network. Multiple data points are collected in real-time to maintain the most efficient functioning of the networks; ticket machines register the number of passengers entering and exiting stations, and sensors record exact transport locations and delays on the network. This is then combined with known information, such as planned maintenance work and scheduled events in the city.

If a metro line has delays, trains can be re-routed or services added on other metro lines. The information could also be relevant for other parties, so that the smart city transport network can as a whole function in the most efficient manner. Information on delays can be sent in real-time to nearby terminals or depots so that

[35]European Commission (2016), p. 4.

[36]Alliance for the Internet of Things Innovation; see also European Commission, https://ec.europa.eu/digital-single-market/en/internet-things. Accessed 10 Jan 2017. AIOTI is now a European Association.

[37]See www.internet-of-things-research.eu/. Accessed 10 Jan 2017.

[38]See https://ec.europa.eu/digital-single-market/en/building-european-data-economy. Accessed 10 Jan 2017.

[39]European Commission (2017).

[40]European Commission (2017), p. 10.

additional buses and trams can be added in relevant places to help ease the congestion. In addition, travellers who have signed up for notifications on their mobile devices could be given an updated route plan, as a result of the delays and updated timetables.

Allowing the different modes of transport to work together would create a smarter system and make sure that travellers are aware of the easiest way to get to their destinations. For this to work, however, those involved in the provision of smart solutions need to share their data. If any property right exists in data or applications created by the IoT, this may be harder to achieve in practice, as property owners can decide whether such data or applications are made available, and at what cost.

3.1 Data as a Property

Property law is one of the oldest rights in legal history. Some claim it even pre-dates the development of human language.[41] The origins of property law, especially in the western world, concern the regulation of scarce resources.[42] In a digital environment, however, bits and bytes are rarely scarce, as data can easily be copied and one person's use of data does not exclude another from using the same data; the latter is referred to as non-rivalrous nature of data.[43] So at least from a technical perspective, data is neither scarce nor rivalrous.[44]

Some have claimed that virtual goods can—through technological measures—be artificially made scarce.[45] In other words, through limiting the availability of e-books, digital music, movies and apps, virtual objects are in practice made scarce.[46] While this argumentation is reasonable when talking about virtual worlds and games, where players can purchase certain objects (a sword, clothing, tools) for money, it does not necessarily apply to data as such, as data is not a closed container of content such as e-books, digital music or apps. Data is, on the contrary, fluid, changes constantly and lacks a counter-part in the tangible world. It therefore is difficult to use the same arguments for data as for virtual property rights on virtual goods, as data has no physical counter-part.

One of the cores of property and the concept of ownership is the right to possess.[47] An important part of this right is the ability to exclude others from

[41]Mattei (2000), p. 4.

[42]Mattei (2000), pp. 1 et seq., see also Malgieri (2016a), p. 5.

[43]See, e.g., Lessig (1999), pp. 130–135.

[44]See also Samuelson (1999), p. 1138; on the related discussion on non-rivalrous nature of goods versus ideas, see Lessig (1999), pp. 130–135.

[45]Lehdonvirta and Virtanen (2010).

[46]Erlank (2013), p. 210.

[47]Clarke and Kohler (2005), p. 180.

possessing one's property.[48] Here arises the first difficulty of possessing "data." Again, as it is easy to copy data it is difficult, in practice, to exclude somebody else from using the same data, unless technical protection measures are set in place and access is limited. Technology has a large impact on how a potential property right can be enforced in practice.

Another traditional part of any property right is the ability to exclude the world.[49] In other words, the right is stronger than many other rights because enforceability is guaranteed against everyone else, not just a contracting partner. The property right is directly based on the law and does not require contractual arrangements between parties.

As there is no harmonization within the EU on property law, individual rights are determined by national legislation in the Member States. Dependent on these national rules, there may therefore be different answers to the legal question of property rights to data. To illustrate this, we will use the examples of Germany, where there has been a rather extensive academic debate on the issue,[50] and the UK, where the courts have ruled on data ownership.

In the German discussions, both civil and penal law have been used to argue for and against a quasi-property right to data.[51] Though Sect. 903 of the Civil Code BGB that regulates ownership has not been interpreted in case law as regards data as "things," legal academics have argued that data could be recognized as a legal interest (Rechtsgut) according to the provisions that regulate liability for damages.[52] From a criminal law perspective, it has been argued that the Penal Code (StGB) could include an indirect right to data, as there are provisions concerning changes to data and computer sabotage in the chapter on damages to objects. After extensive discussions, however, legal academics agreed that this would involve over-stretching the interpretation of existing law. Currently, neither German legislation nor case law explicitly award a property right to data.

In the UK, the Court of Appeal had to decide if data can be subjected to liens.[53] A lien is the right of one person to retain possession of goods owned by another until the owner settles the claims by the possessor. The conclusion of the court was that despite convincing arguments to extend liens to digital material, the wording of the existing legislation could not be interpreted in such a way. The court concluded that it should be left to the legislator to extend the law to include digital material.[54]

---

[48]Clarke and Kohler (2005), p. 180, see also Grützmacher (2016), p. 485.

[49]Purtova (2015), p. 89; Schwartz (2003), p. 2058.

[50]See, e.g., Dorner (2014), Grützmacher (2016), Hoeren (2014).

[51]Hoeren (2014), pp. 753–754.

[52]See Grützmacher (2016), p. 489, cf. Dorner (2014), pp. 617 et seq.

[53]*Your Response* [2014] EWCA Civ 281; [2014]3 W.L.R. 887 at Hert De and Gutwirth (2009), see also Hoeren (2014), p. 752.

[54]Hoeren (2014), p. 752, Kemp (2014), p. 486.

There have been other discussions by scholars on property rights, even from a privacy perspective.[55] One such discussion suggests changing the focus from tangible things to the more dynamic understanding of property as *a bundle of interests*.[56] Based on specific areas of law, it was argued that a property right on (personal) data could be established, while allowing individuals to both share their data as well as limit future uses of the personal data.[57] This would allow the owners of the property right a more fine-tuned right than traditional property law allows.

To summarize the different approaches, one can state that there is currently no explicit property right to data stated in legislation or granted in case law within Europe. The adoption of such a right to include digital information would therefore require clear legislative amendments.

Another challenge in the context of the IoT is *who* should be awarded such a right?[58] Should it be the device manufacturers, sensor manufacturers, software and application developers, infrastructure providers, and/or data analytics companies? Should the right be exclusive to a certain stakeholder or should the relevant stakeholders share any property right?

While the challenge with traditional property law is the fact that data is not a "thing," some other rights might be more suitable for the intangible nature of data. This will be discussed in the following section.

3.2 Copyright and Database Protection

As there is no explicit property right to data, the question arises as to whether any intellectual property rights can be claimed in IoT data, in the form of copyright. If so, the copyright owner can decide how that data is to be used, impacting on IoT solutions.

3.2.1 Copyright in IoT Data

For legal protection in the form of copyright to apply, the concept of originality must be found. In line with international copyright conventions a level of creativity must exist for this to occur; only such works that exceed this (fairly low) quality threshold can be granted copyright protection. In an IoT environment data is created stemming from a number of sources. However, the data is not "created" in the traditional sense: no artistic or literary thought lies behind the data. Rather, the data is collected automatically from an individual or the surroundings in the form of measurements.

---

[55]See, e.g., Samuelson (1999).

[56]Schwartz (2003), pp. 2094 et seq.; referred to in Malgieri (2016a), p. 7.

[57]Schwartz (2003), pp. 2094 et seq.; see for a discussion on the challenges of this approach with regards to personal data from a US perspective, Samuelson (1999), pp. 1138 et seq.

[58]See also Grützmacher (2016), pp. 486–488.

Measurements and automatically created data cannot be said to have such a creative or intellectual element as required by copyright.[59] No artistic or literary judgment has been made, rather data has simply been recorded, time-stamped and stored. Additionally, it is arguably not the IoT provider, but the end-user who in some instances is "creating" the data, for example where an end-user's measurements are being tracked through step-count or heart-rate. Were copyright to exist, a user would therefore own the data and would need to grant a license to any organization wanting to use the data. On the other hand, where the smart object itself creates the data, it could be argued that there is a link with the organization for copyright purposes; this would be the case for example in measuring transport locations and even the number of passengers at a particular location, as no data specific to the individual is being recorded. However, regardless of who (or what) is creating the data, the first copyright hurdle would still not be overcome, namely that no creativity or originality can be found in such "works."

Where no copyright exists in IoT data, none can be claimed by an IoT provider. However, database rights may exist, where legal protection is given based upon how the data is structured, rather than in the data itself. For database copyright, the database itself must pass the originality test i.e., there is originality in the selection or arrangement of the database contents.[60] Alternatively, a reduced level of protection can be given where a substantial investment in the work is shown, known as a sui-generis right.[61] No creativity or originality is needed here, but a sufficient level of time and effort in the structuring of data must be shown; protection can therefore even apply where a significantly large amount of data is involved. This is the most likely form of database protection in relation to the IoT, due to the amount of data and the time and effort involved to ensure the structure facilitates the use of the IoT solution; it is unlikely originality in the selection or arrangement of data could be shown. The sui generis right protects another party from benefiting from the result of the original investment, prohibiting the use of the whole or a substantial part of the contents.[62] The term of protection is shorter than for copyright, but can be renewed where a new investment is made.[63]

To apply this to our scenario, any database rights that do exist would not be an obstacle for the sharing of specific data, either with another transport company or individuals. No substantial parts of the database need to be copied, only what is relevant to the transport company or the mobile application. In addition, it is in practice the company that decides what data to share, and in what form it is provided.

---

[59]See, e.g., Article 2 Berne Convention (1886) for the Protection of Literary and Artistic Works, World Intellectual Property Organisation.

[60]Article 3 Directive 96/9/EC; see also Kemp (2014), p. 487.

[61]Article 7 Directive 96/9/EC. One of the goals of introducting this protection was to reward and protect certain investments that otherwise would not have been protected through copyright law.

[62]Grützmacher (2016), p. 488.

[63]Directive 96/9/EC Article 10; the term is set at fifteen years.

Another form of protection may, however, apply and will therefore need to be considered for IoT solutions. Software protection is granted in accordance with the general copyright provision on originality.[64] If the metro company has created specific software to manage the IoT sensors and collect information within the train and metro system, they own the exclusive right to that software, including its distribution and use. Other entities will therefore not be able to access or use the software without prior agreement, producing a practical obstacle to IoT data sharing. An appropriate solution for a smart transport system may be that companies use the same software; this would facilitate the efficient sharing of data between the train/metro systems and the bus/tram systems. If this is not practically possible, one could create the software and then grant a license to the other to use the software for specific purposes.

As mentioned above, in practice it will be the company itself deciding how data is shared, and so software protection should not be an obstacle to the efficient functioning of IoT solutions. Its creation and usage is, however, an issue that parties need to consider when creating an IoT solution, to avoid any potential legal and practical issues related to the sharing of IoT data.

3.2.2 Copyright in IoT Data Analysis

Legal protection in the form of copyright may also apply further down the line, not in the IoT data itself but in its subsequent collation and analysis. IoT data may be analyzed and evaluated to find trends and patterns in the use of IoT devices, to identify cause and effect triggers, etc. When analysis of IoT data is carried out a work product may result, in the form of for example a report or statistical analysis. Where this product reaches the copyright threshold, discussed above, copyright protection would result.

Copyright protection, however, has a limited value to a company from the perspective of investing in IoT solutions. As protection cannot be given for ideas, only the expression of an idea, this would not prevent others from using an idea and, for example, integrating it into competing IoT solutions. Where companies wish to exclude others from reaping a benefit of their investment, trade secrets may be a better fit in protecting such an analysis.[65]

3.3 Contract Law

With a lack of explicit rights to data from both traditional property law and intellectual property law, many stakeholders use contracts to guarantee a certain

[64]Directive 2009/24/EC Article 1.

[65]See below Sect. 3.5.

minimum level of legal protection. In fact, currently, contractual arrangements seem to be the most common way of regulating potential data ownership and the right to data.[66] While the European Commission considers contractual solutions to be "a sufficient response," it encourages best practices within certain sectors.[67]

The contracting parties will agree through the terms and conditions who has the original right to the data and if there are any potential usage rights linked to the data. For example, the proposed standard contract on Cloud computing by the Swedish IT&Telekomföretagen 2010 stipulates that the customer shall have all the rights to the customer's data.

An advantage of contractual conditions on the right to data is that they are enforceable against the other contracting party and impose strong obligations.[68] For liability to be found a breach of contract must be proven, but the required evidence might be less than for breaches of intellectual property rights. Contracts can give the parties stronger rights than are granted by law, at least between two businesses.

A disadvantage of a right to data based on contract is that, due to privity of contract, it is only enforceable against the other contracting party, and not against any other stakeholders.[69] In an IoT setting the question also arises which contractual agreement outweighs other terms and conditions if there are several contracts between users and device manufacturers, sensor manufacturers, software and application developers, infrastructure providers, and data analytics companies. In addition, contractual rights may loose against other rights explicitly stipulated by legislation, such as personal data rights and in bankruptcy proceedings.

3.4 Bankruptcy Law

Though contractual solutions play an important role, there are certain circumstances where such solutions may not provide sufficiently protection. As there are potentially several stakeholders involved in an IoT environment, some of them may face financial challenges and even bankruptcy. In such cases, the law weighs different claims against each other and stipulates which claims are to be prioritized.

In many countries, some claims are considered preferential and dealt with before contractual claims, such as those with security or where property rights are involved. Depending on the amount of debt that has been accumulated, contractual claims may therefore be settled to a lesser degree or not at all. As data is often the main business asset within many IT companies, especially in an IoT environment, it may also be its main economic value. Selling the data may be the only way to settle

[66]European Commission (2016), p. 21; see, e.g., for the banking sector Kemp (2014), p. 484.

[67]European Commission (2017), p. 10. It is interesting to note that such contractual data ownership conditions are less common in privacy policies for consumer services, see Peppet (2014), p. 144.

[68]Kemp (2014), p. 488.

[69]Kemp (2014), p. 488.

bankruptcy claims. In an IoT setting a related question is if one manufacturer, such as the sensor manufacturer, faces bankruptcy, which of the other stakeholders has the stronger right to the data according to the contract, or will all others have the right to access the data?

While not very common, at least one EU country has acknowledged the legal challenges in a bankruptcy situation and amended its legislation to allow stakeholders a stronger right. In 2013, the Luxembourg Parliament introduced provisions into the Code of Commerce that allow owners of intangible goods held by the debtor in a bankruptcy to reclaim the data at their own expense, provided they are separable from the other assets.[70]

The example, of course, only applies in case of bankruptcy of a stakeholder that has data and not in other cases, so one cannot argue for a far-reaching property right for data. The example shows, however, that such a right could be established in certain situations, depending on the interests and stakeholders involved.

3.5 Trade Secrets

Especially within the IT sector, some inventions or creations are not protectable by intellectual property rights. While copyright and patent protection are used often to protect technological developments, there are various scenarios where they cannot apply, for example the algorithm is not a written code and does therefore not fall under copyright nor is it a technical process that involves hardware and is therefore not patentable. In these cases, especially for algorithms, trade secrets law is being used. For example, Google's algorithms are protected by trade secrets.[71]

Within the EU, trade secret law is harmonized, especially through the recently adopted Know-How Directive.[72] When transposed into national law, by June 2018 at the latest, it will grant protection for the unlawful acquisition, use and disclosure of trade secrets.[73] For information to be regarded as a trade secret, the information must:

(i) Be secret, i.e., not readily accessible to the public;
(ii) Have commercial value;
(iii) Be "subject to reasonable steps…to keep it secret."[74]

[70]Bartolini et al. (2016), Chap. 4.2.

[71]Lohr (2011).

[72]Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.

[73]European Commission (2017), p. 10.

[74]Article 2 Directive (EU) 2016/943.

Data collected within the context of the IoT is generally of commercial value.[75] However, point (i) may constitute a legal challenge, as collected data may be exchanged and shared between stakeholders and therefore not be secret to the extent that is not "readily accessible to persons within the circles that normally deal with the kind of information in question."[76]

Another requirement for trade secrets protection is to *keep the information secret*, which means measures have to be in place to protect the secrecy of information,[77] for example restricting the number of people who have access to the data. In the context of the IoT and Big Data, this poses a practical challenge, as at the point of data collection the data as such is not necessarily secret. The data has to be kept secret through all steps of processing, including collection, storing, and analysis. In practice, keeping secret involves not only technical protection but also contractual agreements and secrecy clauses between different stakeholders.

In the past, collections of data such as client lists and other personal data have been considered trade secrets, as in many cases the data possesses the most business value to a company.[78] The protection was, however, often focused on a finite set of data, not a massive amount of different types of data, collected through multiple devices.

While trade secret protection may be difficult to establish for raw data, especially due to the challenge of "keeping it secret," protection for analysis based on the data is likely to have a bigger chance of protection.[79] Much, however, depends on the stakeholders themselves and the purpose of the data analysis.

3.6 Business Rights to Data in Practice

This section has shown that it is difficult to establish a general property or intellectual property right to data within the EU. Although certain Member States may have developed particular solutions, the identified challenges will most certainly be the same considering that intellectual property rights and trade secrets are harmonized within the EU. In practice, stakeholders will therefore need to rely on contractual agreements, which will not give rights towards third parties as would be the case for property rights; however, stakeholders can at least determine specific rights to the data as between their contracting partners.

One question, however, remains—what is the socioeconomic value of awarding businesses a right to data?[80] While the historic idea of intellectual property awarded

[75] See also Grützmacher (2016), p. 488.

[76] Article 2.1 (c) Directive (EU) 2016/943.

[77] See also European Commission (2017), p. 10.

[78] Malgieri (2016), pp. 102 et seq.

[79] See also Dorner (2014), pp. 622–623.

[80] See Dorner (2014), p. 625.

specific rights to intellectual creations, the reasoning was to give an incentive for investments in new knowledge.[81] For the IoT and Big Data, one can argue that this is not necessary as there is no investment in knowledge; data is simply generated through technological inventions that might themselves be protected by intellectual property, but the data these inventions generate is not necessarily an investment in itself.

4 Right to Data: The Individual Perspective

Most data collected through the IoT will relate to an individual and therefore be considered personal data. While the right to data from a business perspective is slightly unclear, the right to one's personal data has been enshrined in EU legislation since the Data Protection Directive (DPD)[82] and even more clearly through the recently adopted General Data Protection Regulation (GDPR).[83]

The first question to be posed is whether the data can be considered personal data. While this might sound like a basic question, it is of utmost importance for the legality of the *further* processing whether the data can be linked—even indirectly—to an individual. Personal data has been interpreted rather broadly, particularly due to the term "indirectly" stated in the DPD[84] as well as the phrase: "to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person."[85] In other words, the controller does not need to be able to identify a specific person; as long as somebody can recognize a certain individual the data is considered personal.[86] This approach was slightly adapted by the Court of Justice of the European Union (CJEU) in the recent *Breyer* case, as now the assumption is that data is considered personal data if the controller has legal means to access data that enable it to identify a specific person.[87]

The GDPR, however, provides for a limited exception of its application: anonymization. The data protection rules should "not apply to anonymous

[81]Dorner (2014), p. 625, Samuelson (1999), pp. 1139–1140.

[82]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.

[83]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. The GDPR will come into force in May 2018.

[84]Definition of personal data in Article 2 (a) Directive 95/46/EC.

[85]Recital 26 Directive 95/46/EC.

[86]See also Article 29 Working Party (2007).

[87]C-582/14 Patrick Breyer v Bundesrepublik Deutschland, Judgment of the Court (Second Chamber) of 19 Oct 2016.

information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable."[88] Until now, the EU data protection advisory group, the Article 29 Group, has interpreted "anonymized" rather strictly and considers simply removing identifying elements as insufficient, but that the deletion of the original raw data is required as well as other technical measures to ensure that the individual cannot be re-identified.[89] In its opinion on the Internet of Things, the Article 29 Group further underlined the challenges of being completely anonymous in an IoT setting and stated a clear risk of re-identification in the context of IoT.[90]

In conclusion, personal data will be processed in an IoT environment in many, if not the majority of, cases. In the following sections, we will therefore discuss the rights to data from an individual perspective.

4.1 Privacy as a Property

The idea that privacy can be regarded as a quasi-property right has been discussed since the late 1990s.[91] These discussions intensified in the last decade, with the rise of more advanced data collection and data analysis techniques and the gaining importance of personal data as a business asset. Some have claimed that personal data is a "de facto" property in our economy today.[92] As previously mentioned, the business value of many companies today is based on their ability to collect, store, analyze and share personal data. To this extent, personal data is the new currency within the information society.[93]

Some have also argued that the focus of EU legislation on data rather than on privacy gives the impression that the rights concern more the object (the data) than the subject (the individual),[94] strengthening the idea that data protection gives a kind of right to the data instead of protection of an individual. Others have gone as far as to claim that there is a property right regime in the GDPR despite the fact that the regulation is framed from a human-rights perspective.[95] In the following, we

[88]Recital 26 Regulation (EU) 2016/679, which matches Recital 26 Directive 95/46/EC.

[89]Article 29 Working Party (2014a), p. 9.

[90]Article 29 Working Party (2014b), p. 11.

[91]Samuelson (1999), Schwartz (2003), Purtova (2015).

[92]Malgieri (2016a), p. 5.

[93]See Chapter "The Principle of Purpose Limitation and Big Data". This is underligned by an EU proposal suggesting that personal data may be a counter-performance in online contracts, Article 3 European Commission Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content COM/2015/0634 final.

[94]Malgieri (2016a), p. 6.

[95]Victor (2013), p. 515.

will discuss specific aspects of the GDPR that establish, in our view, a rather strong right for the individual to her data.

4.2 Data Erasure

Besides the right to access one's personal data and receive information about which data is stored,[96] the GDPR grants the individual an explicit right to erasure ("right to be forgotten").[97] There are a number of circumstances where this right can be used, including where personal data is no longer necessary, the individual withdraws her consent, or she objects to the processing.[98] There is an exemption concerning freedom of expression, but considering recent case law of the CJEU this has been interpreted narrowly.[99] An individual has a strong right to request erasure of her data, especially considering that the data controller is required to contact other controllers with whom the data has been shared in order to erase the data.[100] In other words, the right of the individual not only concerns the data controller with whom she has had direct contact, and most likely a contract, but also encompasses other parties that have received the individual's data. In an IoT setting, the individual could for example not only request deletion of her data by the device manufacturer, but also the sensor manufacturer, software and application developer, infrastructure provider, and/or data analytics companies. As the user might not have individual contracts with each of them, one could speak of a quasi-property right as the GDPR grants the right even against third parties and goes beyond contractual terms and conditions.

It has been argued that the right to erasure is rather strong,[101] as it not only gives data controllers a limited license to use an individual's data but the individual can change her mind at any time and therefore break the contract with the data controller without any reason by withdrawing her consent. As the right is established by legislation it would override any contractual arrangements that have been made between the individual and the stakeholder. To this extent, the right to erasure weighs stronger than contractual rights.

[96]Article 15 Regulation (EU) 2016/679.

[97]Article 17 Regulation (EU) 2016/679. The DPD established such a right, see Article 12 (b) Directive 95/46/EC.

[98]See Article 17 Regulation (EU) 2016/679. See also Victor (2013), pp. 523–524.

[99]Article 17.3 Regulation (EU) 2016/679. See "Google Spain case": C-131/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Judgment of the Court (Grand Chamber) of 13 May 2014.

[100]Article 17.2 Regulation (EU) 2016/679.

[101]Victor (2013), p. 524.

4.3 Data Portability

Another provision in the GDPR that underlines a strong right to one's data is the newly introduced right to data portability. An individual has the right to "receive the personal data concerning" her, in a structured, commonly used and machine-readable format.[102] This right enables the individual to move her personal data between services[103]; in practice, this should encourage interoperability between services, as stakeholders are more likely to provide the data in the same format.

The right to data portability does not automatically mean that the data should be erased, as these are two separate rights; rather it gives an individual the right to receive one's data in a digital format and not only a list of text. In an IoT setting this means that a user can easily move between different services, for example trying out different smart health solutions, while keeping her data.

The right only applies when the processing is based on the consent or a contract between the individual and the controller.[104] We assume that this would be the case in most IoT settings. While the right to data portability is not as strong as a property right it does establish a kind of right to data, as it concerns possession of one's property, even though the possession is not exclusive.

4.4 Data Protection as a Right to Data

EU legislation, through the DPD and the GDPR, explicitly stipulate certain individual rights: access to *information about* the data, *access to* the actual data, and last but not least a right to request *erasure of* the data. Taken together these three specific rights establish a rather strong right for an individual to access her own personal data.

A potential challenge in an IoT setting is to identify who has one's personal data to start with: the device manufacturer, sensor manufacturer, software and application developer, infrastructure provider, and/or data analytics companies. Another is that not all data is linked to the individual, meaning it cannot be considered personal data. Data that was originally collected from an individual may change its status over time through anonymization or pseudonymization techniques; the flipside of the business incentives to anonymize or pseudonomize personal data results in a diminished right to the data itself from an individual perspective.

[102] Article 20 Regulation (EU) 2016/679.

[103] Article 29 Working Party (2016), p. 4.

[104] See Recital 68 Regulation (EU) 2016/679.

One advantage of the data protection provisions, however, is that stakeholders have strong obligations to protect the data; this is the subject of the following section.

5 Protection of Data

As has been shown in the previous chapters, certain rights to data may apply in an IoT context, both from a business and individual perspective, with legal remedies available where those rights are infringed. Reliance on the law is, however, not the only way to protect IoT data. Technical measures can also be used in the interests of individuals and stakeholders to physically protect the data. In some cases, the law requires a certain level of security in the form of technical and organizational measures; this is particularly the case in relation to personal data, where appropriate measures must be implemented to protect the privacy rights of a data subject.[105] There are, however, other reasons for organizations to secure data using technical means. As more worthwhile data is produced from the use of IoT solutions, data security also becomes more important from a business perspective. This is not only due to the potential impact data loss can have on an organization's reputation, but also because of the increased need for stakeholders to protect their own business interests in the data, for example through trade secrets.[106]

For example, let us use the scenario of a smart manufacturing company that has a large database with information relating to warehouse stock and sales.[107] Analysis of the collected data has revealed trends in the company's stock, with certain products in demand at particular times of the year. The company can use this Big Data analysis to streamline manufacturing, saving on warehouse costs. The result of the analysis, together with information stored in its database, is of high value to the company. It therefore wants to make sure that no unauthorized person gains access to the data, that it cannot be tampered with and is kept confidential from competitors. Technical protection of the IoT infrastructure is therefore of great importance to the company.

5.1 Challenges of IoT

Particular challenges exist in protecting data in the IoT environment, due to the amount of data involved and the nature of IoT solutions, something which must be considered when deciding upon appropriate security measures. Firstly, the amount

[105] Article 17 Directive 95/46/EC.

[106] See above Sect. 3.5.

[107] See above Sect. 2.3.

and type of data created, coupled with the possible inferences that can be drawn from multiple data points leads to a need for comprehensive protection. Secondly, data must be protected in various places as the IoT environment is reliant on data sharing and Internet connectivity[108]: devices themselves must be sufficiently secure and data must be protected when stored and communicated, whether this is within a user's local network, transferred to a business or uploaded to the Cloud. Thirdly, multiple actors are often involved in the creation of IoT solutions; therefore, in order for data protection and security measures to be effective, the various stakeholders involved in the development, production, and deployment of the IoT must work together.

The first two challenges focus on the security of data and devices. The regularity with which IoT data is created, transferred and stored at multiple locations leads to a need to protect both data in rest i.e., stored locally or otherwise, and data in motion i.e., transferred from one location to another via a network. End-to-end encryption of data is of course a good starting point. However, IoT solutions must also consider organizational aspects such as who has access to the data, how this data is processed and analyzed, and in what form. In addition to securing data, focus needs to be placed on the physical infrastructure and devices that make up the IoT in order to secure and authenticate the various sensors, trackers and appliances. In practice, a secure infrastructure can be challenging, as although most IoT applications have some form of physical interface, these can often be very small. This may impact on security procedures, for example secure log-in not possible on the device itself will need to be carried out remotely from another, connected, device.

The third challenge focuses on the security of different parts of an IoT solution. To work seamlessly, all parts must work together, or be "interoperable" to provide a valuable service to the end-user. The IoT entails "complex and sophisticated interdependencies both within products (based on hardware and software) and across interconnected devices."[109] This interoperability principle also applies to security; security protocols must be compatible with each other and all parts of an application should adhere to the same level of security (security is only as strong as its weakest link).[110] This challenge relates to the interacting parts of any IoT solution, but is of course greater where a number of stakeholders are involved.

The challenges in providing a secure IoT environment are, however, not completely unique in nature. Similar issues have been encountered in the fields of, for example, Cloud computing and radio frequency identification (RFID). IoT providers can therefore use developments and solutions relating to other technologies as an inspiration for the IoT. For example, the Article 29 Group provided practical guidance to users and providers of Cloud computing, based on applicable data protection obligations.[111] As the transfer and storage of a large amount of data

[108]Gerling and Rossow (2016), p. 507.

[109]European Commission (2017), p. 4.

[110]Article 29 Working Party (2014b), p. 9, Shackelford et al. (2017), p. 14.

[111]Article 29 Working Party (2012).

is common to both Cloud computing and the IoT, similar measures to protect data may be suitable. In the area of RFID, which can be viewed as an important pre-cursor to the IoT environment, privacy and security challenges have been highlighted by many, including the OECD and the EU.[112]

In an EU legislative context, there has not been any attempt to draw up specific legislation on the protection of data in an IoT context. Nor does there appear to be any need, due in part to the fact that many of the challenges are not IoT-unique. As the EU legislation is of an over-arching nature, the same rules can be applied to the IoT environment. In other jurisdictions, where a more sector-specific approach to privacy and the protection of data is taken, legislation focusing on the IoT may be more appropriate. To illustrate this, a bill was recently proposed in the US to introduce security regulations specifically for motor vehicles.[113]

5.2 *Security Breaches and Data Loss in IoT*

As new technologies and solutions for large amounts of data have been introduced, data loss has stood out as a particularly important issue. The individual rights to data that exist are only relevant if an individual can make use of them.[114] Where data is lost, many of the protections provided for in the law would be unenforceable in practice. As data increases in economic value, both individuals and businesses have an interest in avoiding data loss. Particularly in the IoT environment, where so much data is involved, there are therefore legal and economic arguments for keeping data safe. Widespread security breaches involving data loss or unauthorized access to data would also likely threaten IoT growth and innovation.

A recent example of an IoT security breach was the attack on DNS provider Dyn in October 2016. Here, IoT devices were one of the sources of a distributed denial-of-service (DDoS) attack after being infected with malware; as a result, many high-profile news and entertainment websites and services became unavailable. Although the attack did not focus on user data, it is apparent that the security measures being used by certain IoT devices were lacking. Similar attacks could abuse the security flaws and, instead of using IoT devices as conduits, rather focus on theft and exploitation of personal data, for purposes such as profiling of individuals, credit card fraud or identity theft. Other IoT security breaches have been of a more theoretical nature, revealed through hacking "contests" where the aim is to

[112]OECD (2008); European Commission Recommendation 2009/387/EC of 12 May 2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification.

[113]Security and Privacy in Your Car Act S-1806, introduced into the US Senate in July 2015; also referred to as the "SPY Car Act."

[114]See above Sect. 4.

find flaws in new technologies and solutions, and through studies of specific smart devices available on the market.[115]

Such security breaches and threats have lead to increasing concerns relating to security flaws and data loss in the IoT, sometimes from surprising sources, for example the US Department of Homeland Security.[116] Less surprisingly, large companies involved in IoT solutions have also focused on security issues. Volkswagen recently announced it was cooperating in establishing a new automotive cyber security company "to make vehicles and their ecosystem more secure."[117] Interesting to note is that this followed a well-publicized flaw in car remote control security systems (including Volkswagen's), allowing unauthorized access to vehicles.[118]

As more companies are becoming aware of security issues of smart technology, better security solutions are likely to be incorporated into products and services, particularly where there is a potential impact on a company's reputation and trustworthiness. However, not all IoT solutions currently have effective security measures, as shown by recent security flaws, such as those mentioned above.

Formal legal consequences of losing data have traditionally been limited in nature; standard contractual clauses have been applied, leaving end-users in a weak position unable to negotiate more stringent protections. Data loss has, however, now become a focus of EU legislation. New obligations will be introduced under the GDPR relating to a personal data breach, defined as a security breach involving "the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."[119] In such circumstances, an organization has an obligation to inform the relevant data protection supervisory authority within 72 h.[120] Organizations that do not have proper procedures in place can be fined by the supervisory authority, either in the form of a fixed fee or based on their (global) annual turnover.[121] Previously, data protection authorities have not had such enforcement powers, acting rather in an advisory capacity.

Although it is not yet known whether supervisory authorities will use these powers to their fullest extent, it is clear the consequences of losing user data in the EU will be greater. Contractual clauses will still be of importance in relation to the individual user, as the fines given are purely of an administrative nature; regulation of individual remedies in the form of damages has been left to each Member State. The new legal provisions are, however, likely to provide additional incentives to organizations involved in large-scale data processing, including in an IoT context, to implement effective security solutions to minimize the possibility of data loss.

---

[115]Peppet (2014), pp. 165–176.

[116]US Department of Homeland Security (2016).

[117]Volkswagen (2016).

[118]Garcia et al. (2016).

[119]Article 4 (12) Regulation (EU) 2016/679.

[120]Article 33 (1) Regulation (EU) 2016/679.

[121]Article 83 Regulation (EU) 2016/679.

5.3 Security Requirements in an IoT Context

In accordance with the current EU Data Protection Directive (DPD) an "appropriate" level of security must be provided by an organization, both through technical and organizational means where personal data is involved. Organizations must carry out a risk analysis, taking into account the technical possibilities that exist, the cost of security measures, the risks of data processing and the type and amount of data that is involved in any processing.[122] EU law therefore requires companies to consider the effect of data processing in their operations and to react accordingly in order to protect an individual's data.

The GDPR builds on the existing obligations of the DPD and heightens the onus on organizations to consider legal aspects at an early stage in the development of a product or service, both from a security and data protection perspective. As a result, a number of current best practices are being incorporated into law:

(i) *Data protection impact assessments (DPIA)*[123]: proactive measures in the form of risk assessments required where personal data is processed, particularly in cases where new technology is being used;
(ii) *Data protection by design*[124]: the principle that data protection is to be built into a system from the design phase. Appropriate measures need to be implemented to adhere to the data protection principles and protect the rights of data subjects;
(iii) *Data protection by default*[125]: appropriate measures need to be implemented to ensure only necessary personal data is processed and shared;
(iv) *Breach notification*[126]: an organization's obligation to inform an authority and/or the data subject when a data breach occurs.

The changing status of these principles to formal legal requirements means that providers, including those involved in IoT solutions, will need to adhere to more specific security requirements in the future. The principles all have an impact on which security measures are appropriate in a given IoT situation. *DPIAs* are especially useful where dealing with new technology, as some impacts may not initially be known, and personal data is often processed in a routine manner. IoT solutions can be very personal in nature, especially in the area of smart health and smart homes, where an individual's movements, biology, fitness and daily routines are measured and analyzed, making DPIAs vital to the IoT environment. An assessment of the related risks is therefore required to provide an appropriate security level at the various locations. Inspiration for carrying out such assessments can be found in various places; for example, a DPIA template for smart grids and

[122] Article 17 Directive 95/46/EC.
[123] Article 35 Regulation (EU) 2016/679; also known as privacy impact assessments or PIA.
[124] Article 25 (1) Regulation (EU) 2016/679; also known as privacy by design.
[125] Article 25 (2) Regulation (EU) 2016/679; also known as privacy by default.
[126] Articles 33–34 Regulation (EU) 2016/679; see above Sect. 5.2.

metering systems[127] and a DPIA framework for RFID applications[128] have been developed.

Once such a risk assessment has been carried out, IoT developers are in a position to think about *data protection by design* and *data protection by default*, building in privacy to the system from the outset. Limiting the amount of data collected may seem a little backward-thinking in relation to the IoT, where massive volumes of data are collected. However, the data minimization principle is still of relevance. For example, some information may not need to be collected or shared as initially planned, or the user can be given a choice over which data is processed, based on their functionality needs.

These three principles should, therefore, be considered at an early stage in the development of an IoT solution. They may also need to be returned to at a later stage, when circumstances change. For example, where additional functionalities are added to an IoT product or service, a new DPIA will be needed as the risks may have changed.[129]

Breach notification also has an impact on security measures, as in order for an IoT organization to inform an authority or an individual of a data breach there must be measures of a technical and organizational nature in place. For example, it must be clear when a breach has occurred, what information is involved in the breach, and who the responsible person is within the organization to inform the relevant people about the breach.[130] Security measures should also be put in place to stop such a breach from occurring again.

The GDPR provides more detail on the types of security measures organizations are expected to carry out, depending upon the risk of the data processing.[131] For example, pseudonymization and encryption of data are explicitly mentioned, along with testing and evaluation of security measures.[132] These provisions strengthen individuals' rights, as data should be stored using robust security measures. However, the provisions may also lead to an increase in data pseudonymization or anonymization where a large amount of data is being processed, such as in an IoT environment; where this results in data no longer being identifiable there will be an impact on the individual's ability to access their own data. As it can no longer be connected with the individual, the data cannot be erased, corrected or moved to another service, meaning that the legal protections for the individual[133] can no longer be relied upon. In an IoT context, stakeholders may still have a possibility to

[127]European Commission (2014).

[128]European Commission (2011).

[129]Article 35 (11) Regulation (EU) 2016/679.

[130]The specific requirements in relation to breach notifications are found in Article 33 (3) (5) Regulation (EU) 2016/679.

[131]Article 32 Regulation (EU) 2016/679.

[132]Article 32 (1) (a), Article 32 (1) (d) Regulation (EU) 2016/679.

[133]See above Sect. 4.

benefit from the data, through Big Data analytics, but not the individual who has used the particular IoT solution.

Notwithstanding this potential threat to individual rights to data, the principles and proactive measures in the new EU framework do provide clear guidelines for IoT providers, facilitating the chain of development where a number of providers are involved. The GDPR also provides incentives for companies to protect individual data, as where an organization fails to adhere to the security provisions, fines of up to €10,000,000 or up to 2% of a business' global annual turnover can be imposed.[134]

The main incentive for IoT providers to protect IoT data is, besides where required by law, to protect reputation and trust in their services. As legal repercussions of data loss have generally been of a contractual nature, only the most serious breaches have received media attention. The new EU legal framework has the potential to bring more attention to such breaches, although much depends on the supervisory authorities' practical use of the enforcement powers bestowed upon them by the GDPR.

5.4 Protecting IoT Data in Practice

Protection of data is traditionally considered from a data subject's perspective. EU legislation states the legal obligations where personal data is involved, setting out detailed rules for appropriate security measures. This legislation, although initially a hurdle for IoT stakeholders, has the potential to result in a more secure IoT.

In an IoT context however, the value of the data means that there are clear organizational benefits, and potential legal protections, of protecting both data and infrastructure.[135] Protecting IoT data in practice is therefore likely to become more of a focus for stakeholders. Aware of the lack of a property right in data and the limited scope of intellectual property rights, stakeholders are more likely to focus on other protective measures for the data. To be afforded protection under trade secrets law, one of the requirements is that access to the information must be limited[136]; securing the data through technical means is in practice the only way that this can be done. There are therefore clear incentives for stakeholders to protect IoT data notwithstanding the legal requirements related to the processing of personal data.

[134]Article 83 (4) (a) Regulation (EU) 2016/679. The higher fines, of up to 20,000,000 €, or 4% of a business' global annual turnover, are for more basic infringements, such as data processing principles, data subject rights and transfers of data to a third country, in accordance with Article 83 (5).

[135]See above Sect. 3.

[136]See above Sect. 3.5.

6 Current Status and Future Development

6.1 Right to Own Data Versus Right to Another's Data

As has been shown, the current EU legal framework does not provide businesses with a clear right to the data they collect. There may be specific provisions protecting an analysis based on the original data (copyright or trade secrets) or protecting the data as a whole (database protection). To a large degree, businesses are left to contractual solutions; these provide a strong protection against the contracting partner but are weak against any third party who also has an interest in the data. On the other hand, data protection rights are clearly established in EU law. Rights regarding one's personal data (right to information, data erasure and data portability) and duties of stakeholders processing such data are expressly mentioned in the legislation. Considering these circumstances, it can be concluded that individual rights are stronger than potential business rights,[137] particularly as individual rights cannot be contracted away.

EU legislation has also answered the question of whether trade secrets or data protection weighs stronger. Though the GDPR stipulates that the right to data "shall not adversely affect the rights and freedoms of others,"[138] it also states that "the result of those considerations should not be a refusal to provide all information to the data subject."[139] The Know-How Directive confirms this view, as it states that trade secret protection shall not affect "the rights of the data subject to access his or her personal data being processed and to obtain the rectification, erasure or blocking of the data."[140] So, even if a company protects data collected through IoT solutions, it can never refuse the individual access to her own data.

Another question that arises is whether assigning a property right may lead to other legal difficulties, such as within competition law. It may not always be clear whether any right to data should be awarded to one stakeholder or several stakeholders. The Max Planck Institute for Innovation and Competition recently stated that it does not see a need nor a justification for exclusive rights, as there is "no legal principle that rights in data must be allocated to a specific legal subject from the outset."[141] Neither did it see economic reasons for doing so, due to "the risk of interference with the freedom to conduct a business and the freedom to compete."[142]

[137] See, e.g., Grützmacher (2016), p. 486.
[138] Article 20.4 Regulation (EU) 2016/679.
[139] Recital 63 Regulation (EU) 2016/679.
[140] Recital 35 Directive (EU) 2016/943.
[141] Drexl et al. (2016), p. 2.
[142] Drexl et al. (2016), p. 2.

6.2 Right to Data Versus Protection of Data

Although security measures are only prescribed by law in relation to personal data and not for other data rights, such measures can be a practical aid in protecting business assets such as trade secrets. The law does provide guidance on appropriate security measures in relation to individual rights to data, and therefore seems to lead to a fairly balanced approach between the right to data and the protection of data.

Despite the conclusion that a property right to data from a business perspective is difficult to establish on legal grounds, there are reasons for businesses to invest in a secure infrastructure where large amounts of data are involved.[143] The lack of specific legal provisions for these purposes, however, means that details are lacking on appropriate security measures to protect business interests. This means that, in practice, it falls to each organization to decide upon levels of security. As more companies realize the potential benefits of proactively protecting data, the current balance of rights and duties may be altered. An organization's security measures are often not known unless a security breach or infringement of rights has taken place, and the level of security organizations deem appropriate and sufficient may well differ. There are potential problems with this somewhat flexible approach, as measures may impact on an individual's ability to access their own data.[144] Similarly, other business interests may be threatened due to inaccessible data; one stakeholder could exclude others by using particular technical measures.

It is interesting to note that one reason a traditional property right on data may not be possible is because data can easily be copied and shared without taking away someone else's access; it is not "scarce," as such. However, data may fall within this description if companies do in fact protect data to such an extent that it is no longer available to anyone else.[145] If this were to happen, the legal discussion on the right to data would need to be re-examined.

From an IoT perspective, exclusion of other stakeholders is arguably not an imminent threat, as so much of the environment is built upon interoperability and the sharing of data. However, it is still a relevant concern in avoiding monopoly-like positions on the market. How and the extent to which data is protected is an important aspect of IoT innovation, particularly for start-up companies and others with limited resources or experience within the field but that want to be on the same footing as other IoT providers.

[143] See above Sect. 5.

[144] See above Sect. 5.3.

[145] See Malgieri (2016a), p. 5.

6.3 *Right to Data Versus Open Access*

The lack of a clear legal right to data has the potential of being abused. Stakeholders are in a strong position to exercise their limited legal rights, and it is possible that some will try to extend these rights. A quasi-practical right to data could be the result of such an abuse, through the physical protection of data and the exclusion of others, as mentioned above. It can, therefore, be questioned whether the current framework in fact encourages innovation and market growth.

Another approach can be witnessed at an EU level, where the trend is focused towards open access to data gathered via the IoT.[146] As the EU's aim is to foster a digital single market and an open flow of data to ensure competitiveness on a global level, restrictions to data access are discouraged as they would hamper technological development. The EU is therefore planning to initiate a dialogue with Member States and stakeholders on a potential EU framework for data access.[147]

These two approaches clearly contradict one another. If such an open access approach is to be adopted within the EU in the near future, business rights to data cannot be extended and any abuse of existing rights should be prevented. The balance between open access and protection of individual privacy may, however, be a challenge.

References

ABI Research (2013) More than 30 billion devices will wirelessly connect to the internet of everything in 2020. Press Release. 9 May 2013

Article 29 Working Party (2007) Opinion 4/2007 on the concept of personal data. Available via European Commission. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm. Accessed 16 Jul 2017

Article 29 Working Party (2012) Opinion 05/2012 on cloud computing. Available via European Commission. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm. Accessed 16 Jul 2017

Article 29 Working Party (2014a) Opinion 05/2014 on anonymization techniques. Available via European Commission. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm. Accessed 16 Jul 2017

Article 29 Working Party (2014b) Opinion 8/2014 on the recent developments on the internet of things. Available via European Commission. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm. Accessed 16 Jul 2017

Ashton K (2009) That 'Internet of Things' Thing. RFID Journal. 22 June 2009. http://www.rfidjournal.com/articles/pdf?4986. Accessed 10 Jan 2017

Bartolini C et al (2016) Cloud providers viability: how to address it from an IT and legal perspective? Economics of grids, clouds, systems, and services. In: Altmann J et al (eds) International Conference on Grid Economics and Business Models (GECON), Cluj-Napoca, September 2015. Lecture notes in computer science, vol 9512. Springer International Publishing, p 281

[146]See, e.g., European Commission (2017), pp. 10–11.

[147]European Commission (2017), p. 11.

Bradley J et al (2013) Embracing the internet of everything to capture your share of $14.4 trillion. Cisco, http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoE_Economy.pdf. Accessed 10 Jan 2017
Cisco (2013) The internet of everything and the connected athlete: this changes … everything. http://www.cisco.com/c/en/us/solutions/collateral/service-provider/mobile-internet/white_paper_c11-711705.html. Accessed 10 Jan 2017
Clarke A, Kohler P (2005) Property law: commentary and materials. Cambridge University Press, Cambridge
Custers B, Uršič H (2016) Big data and data reuse: a taxonomy of data reuse for balancing Big Data benefits and personal data protection. International Data Privacy Law 6(1):4–15
De Hert P, Gutwirth S (2009) Data protection in the case law of Strasbourg and Luxemburg: constitutionalisation in action. In: Gutwirth S et al (eds) Reinventing Data Protection?. Springer, Dordrecht
Dorner M (2014) Big Data und "Dateneigentum." Computer Und Recht 9:617–628
Drexl J et al (2016) Data ownership and access to data—position statement of the Max Planck Institute for Innovation and Competition of 16 August 2016 on the current European debate. Max Planck Institute for Innovation and Competition Research Paper No. 16-10
DuBravac S (2014) A hundred billion nodes. Five technology trends to watch 2014. Consumer Electronics Association, pp 3–8
Erlank W (2013) Books, apps, movies and music–ownership of virtual property in the digital library. Eur Prop Law J 2(2):194–212
Ernst and Young (2015) Becoming an analytics-driven organisation to create value. http://www.ey.com. Accessed 10 Jan 2017
European Commission (2011) Privacy and data protection impact assessment framework for RFID applications. 12 Jan 2011
European Commission (2014) Data protection impact assessment template for smart grid and smart metering systems ('DPIA template'). Expert group 2 smart grid task force. 18 Mar 2014
European Commission (2016) Commission staff working document, advancing the internet of things in Europe, SWD(2016) 110 final
European Commission (2017) Building a European data economy, communication from the commission to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions, COM(2017) 9 final
Garcia et al (2016) Lock it and still lose it—on the (In) security of automotive remote keyless entry systems. In: Proceedings of the 25th USENIX security symposium 2016, pp 929–944
Gartner (2016a) Forecast: wearable electronic devices, Worldwide. 19 Jan 2016
Gartner (2016b) Top strategic predictions for 2017 and beyond: surviving the storm winds of digital disruption. 14 Oct 2016
Gerling S, Rossow C (2016) Angreiferjagd Im "Internet Der Dinge." Datenschutz Und Datensicherheit 8:507–510
Grützmacher M (2016) Dateneigentum – Ein Flickenteppich. Computer Und Recht 32(8):485–495
Hoeren T (2014) Big data and the ownership in data: recent developments in Europe. Eur Intellect Prop Rev 12:751–754
IDC and TXT Solutions (2014) SMART 2013/0037 Cloud and IoT combination, study for the European Commission
Kemp R (2014) Legal aspects of managing big data. Comput Law Secur Rev 30(5):482–491
Kuneva M (2009) Keynote speech of the former European consumer commissioner, roundtable on online data collection, targeting and profiling. SPEECH/09/156. Brussels. 31 Mar 2009
Lehdonvirta V, Virtanen P (2010) A new frontier in digital content policy: case studies in regulation of virtual goods and artificial scarcity. Policy Internet 2(3):7–29
Lessig L (1999) Code: and other laws of cyberspace. Basic Books, New York
Lohr S (2011) Google schools its algorithm. New York Times. 5 Mar 2011
Malgieri G (2016a) "Ownership" of customer (big) data in the European Union: quasi-property as comparative solution? J Internet Law 2016:3–18

Malgieri G (2016b) Trade secrets v personal data: a possible solution for balancing rights. Int Data Privacy Law 6(2):102–116
Manyika J et al (2013) Disruptive technologies: advances that will transform life, business, and the global economy. McKinsey Global Institute
Mattei U (2000) Basic principles of property law: a comparative legal and economic introduction. Greenwood Publishing Group, Westport
Organisation for Economic Cooperation and Development (OECD) (2008) Committee for Information, Computer and Communications Policy (ICCP). RFID radio frequency identification OECD policy guidance: a focus on information security and privacy applications, Impacts and Country Initiatives
Peppet SR (2014) Regulating the internet of things: first steps toward managing discrimination, privacy, security and consent. Texas Law Rev 93:85–176
Purtova N (2015) The illusion of personal data as no one's property. Law Innov Technol 7(1): 83–111
Rose D (2014) Enchanted objects: design, human desire, and the internet of things. Scribner, New York
Samuelson P (1999) Privacy as intellectual property? Stanford Law Rev 52:1125–1151
Schwartz Pa M (2003) Property, privacy and personal data. Harvard Law Rev 117:2056–2128
Shackelford et al. (2017) When toasters attack: a polycentric approach to enhancing the 'security of things'. University of Illinois Law Review (forthcoming) https://ssrn.com/abstract=2715799. Accessed 10 Jan 2017
US Department of Homeland Security (2016) Strategic principles for securing the internet of things (IoT). 15 Nov 2016
Verizon (2015) State of the market: the internet of things 2015. http://www.verizonenterprise.com/resources/reports/rp_state-of-market-the-market-the-internet-of-things-2015_en_xg.pdf. Accessed 16 Jul 2017
Victor JM (2013) The EU general data protection regulation: toward a property regime for protecting data privacy. Yale Law J 123(2):513–528
Volkswagen (2016) Volkswagen enters into cooperation with top Israeli experts to establish an automotive cyber security company. Press Release. 14 Sep 2016

Right to be Forgotten: A New Privacy Right in the Era of Internet

Yuriko Haga

Abstract The right to be forgotten is a new right proposed in the context of information society. Reactions to this right vary from country to country because the concept and rationale are not clearly fixed yet. The absence of a consensus on this point has the potential to create uncertainty in an information society that is becoming borderless. Country-specific decisions are not enough for the smooth development of this concept and there is an urgent need to reach a consensus around core points. The starting point of the argumentation here is whether the right to be forgotten is a part of the right of privacy or a totally different right. In spite of some differences, the chapter argues that the right should be deemed an extension of privacy. However, because understandings on the concept of privacy itself are not harmonized, there is a confrontation between countries, specifically between European countries and the United States. The concept of privacy was born at the end of the nineteenth century and countries have developed it taking into account their own fundamental values. However, because of the borderless character of society today, the conflict between fundamental values, notably the privacy to protect the dignity of the individual versus the right to know to guarantee freedom of expression, comes to the surface. This conflict is one of the traditional issues related to privacy and is particularly serious when contemporary societal changes are not taken in consideration. This blocks the possibility of a consensus on the ideal concept of privacy today. An analysis on the right to be forgotten clarifies traditional questions on privacy and it may also be necessary to modify the general theory itself. At the end, the chapter focuses on the current situation of the right to be forgotten in Japan.

Keywords Right to be forgotten · Privacy · Internet · Information · Personal data

Y. Haga (✉)
Faculty of Law, Kanazawa University, Kanazawa, Japan
e-mail: yuriko.haga@gmail.com

M. Corrales et al. (eds.), *New Technology, Big Data and the Law*,
Perspectives in Law, Business and Innovation, DOI 10.1007/978-981-10-5038-1_5

Contents

1 Introduction

Information holds great importance in today's world and its treatment is of considerable public concern.

Today, one of the most actively discussed issues in the legal field is the right to be forgotten. This right is presented in the context of the deletion of information previously collected by any operator. The right holder is a person whose information is in question (the *data subject*).

The discussion about the right to be forgotten is tangled. This chapter aims to examine this situation and to theorize this new-born right. For this purpose, the chapter will first review the concept and development of the right to be forgotten (Sect. 2). Section 3 will then survey dissenting voices regarding this right. Section 4 focuses on the next phases and challenges to the right to be forgotten. The chapter concludes by clarifying the future agenda on the right to be forgotten in Japan (Sect. 5).

2 The Right to Be Forgotten: An Extended Privacy Right in an Online World

On July 12, 2016, a decision of the Tokyo High Court delivered a shock to Japanese society. The decision indicated a change in attitude toward the right to be forgotten on the part of Japanese courts. Although prior decisions from lower courts had initially recognized this "new right," the High Court took a different view.

The High Court decided that the deletion of information from the Internet should be examined under the framework of traditional privacy theory, stating that "Japanese legislation is unaware of the existence of a so-called right to be forgotten…The requirements and the effect of this right remain unclear…" (translated by the author).

Since no other court decision has followed this decision, it is now generally understood that the right to be forgotten is not recognized in Japan. The reason for this is that the control of information spread on the Internet can be covered by the existing right of privacy.

As mentioned in the decision, the concept of the right to be forgotten does remain vague and abstract. In particular, is the right to be forgotten different from existing privacy rights? If so, what is the difference? This chapter begins with an analysis of this point. For that, this section will first confirm the content of the right to be forgotten and its development.

2.1 Development of the Right to Be Forgotten

The right to be forgotten, sometimes called the "right of oblivion" (literally translated from the French terminology "droit à l'oubli"), is one of the "newly-born rights" created by the arrival of the digital age. Today, in information society, a great deal of information is in digital form. Information about individuals has great importance and is collected and stocked, in national & local government database, in companies' caches, or in social network services. Much of this data is being created without users even noticing and it has the potential, in some cases, to damage the reputation of users. Over time, this information can become obsolete, but it still has the potential, at any point, to cause damage to that user and become an obstacle their life.

A typical case is that of the "drunken pirate." A 25-year-old American university student,[1] Stacy, posted a photograph of herself drinking at a costume party on her page of Social Networking Service (SNS). The problem was that she was training to be a high school teacher and her supervisor found the photo. It was deemed unacceptable by the supervisor, who judged the behavior in the photo to be "unprofessional." Furthermore, because the photo seemed to be promoting drinking to students, the university refused to confer a teaching degree on Stacy.

Prior to the arrival of the Internet, the "life" of information was finite. Over the course of time, the public would eventually *forget* the information. However, with the Internet and digital technology, the world has forgotten how to forget. Information is captured and preserved on the Internet and the public can easily access that information with a single click.

[1]Rosen (2010).

Against this backdrop, the right to be forgotten has been proposed. Based on this right, one can make a claim to have such information erased (for example, text or pictures published on the Internet) if the person does not wish that information to be retained.

In 2009, a legislative proposal in France about privacy in a digital age contained the "right to digital oblivion (droit à l'oubli numérique)."[2] Although some preceding cases are found,[3] this was the first appearance of the right to be forgotten in legislation. Therefore, France is often considered as the origin country of the right to be forgotten,[4] although the proposal was eventually rejected and never entered into law.

The European Union has a long history of dedication to the protection of personal information because it is considered as one of the fundamental values recognized by the European Union. A measure that has played a significant role in the protection of personal information is the 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 (hereinafter "Data Protection Directive"). It should be noted that the Data Protection Directive, in itself, does not provide for the right to be forgotten.

The expression "right to be forgotten" became more widely known after the publication of a report entitled "A Comprehensive Approach on Personal Data Protection in the European Union" (COM (2010) 609). This report clearly used the expression and defined it as the "right of individuals to have their data no longer processed and deleted when they are no longer needed for legitimate purposes."[5]

As mentioned previously, there is no written rule in EU legislation about the right to be forgotten. However, the development of Internet technology has heightened the necessity of the right to be forgotten. People are now more concerned about the spread of personal information on the Internet.

Under such circumstances, in 2012, to keep pace with the development of the information society, an amendment of the Directive was proposed (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; COM (2012) 11 final).

In Article 17 of this proposal, the right to be forgotten was clearly mentioned. After discussion, however, the expression "right to be forgotten" was omitted from the final proposal and only the "right to erase" remained. Several reasons for this omission were mentioned. For example, the right is substantively the same as the right to erasure, people can delete information about themselves within the existing

[2]Proposition de loi visant à mieux garantir le droit à la vie privée à l'heure du numérique, Sénat session ordinaire de 2009–2010, No. 93, p. 8.

[3]Carter (2013), pp. 24 et seq., shows the first case of the right to be forgotten in Argentina, *Da Cunha Virginia v. Yahoo & Google*.

[4]Rosen (2012a).

[5]COM (2010) 609, p. 8.

framework, and that the right to be forgotten is not well-defined and its scope remains unclear.

However, the final official text of Regulation 2016/679 (hereinafter "Data Protection Regulation"), which repeals the Data Protection Directive, published in the EU Official Journal on 4 May 2016, contained the right to be forgotten. As it entered into force on 24 May 2016 and will apply from 25 May 2018, it can be pointed out that—at least, in the European Union—the right to be forgotten is clearly recognized today.

The case that lead to this situation is the well-known judgment of the Court of Justice of the European Union (CJEU) of 13 May 2014 (C-131/12, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González).[6]

The facts were as follows. In 2010, a Spanish national, Mr. González (hereinafter "González"), sought a remedy from the Spanish Data Protection Agency (Agencia Española de Protección de Datos, "the AEPD") against a Spanish newspaper company Vanguardia Ediciones SL ("the Vanguardia"), Google Spain and Google Inc.

González claimed that when his name is "Googled," an article published in the newspaper of the Vanguardia from 1998 is shown. The article concerned the seizure and the auction of his property for non-payment of social security premiums. González claimed that the problem had been settled long ago and that the article should be deleted from the website in order to maintain his honor. The AEPD rejected the claim of González against the Vanguardia for the reason that the article had been published lawfully. However, the AEPD ordered Google Spain and Google Inc. to delete the information in question from their indexing database.

Google Spain and Google Inc. filed a suit in court challenging this decision of the AEPD. During the court process, the Spanish court sent a request for a preliminary ruling on the interpretation of the Data Protection Directive to the CJEU.

Preceding the judgment of CJEU, the opinion of Advocate General Jääskinen was delivered on 25 June 2013. The Advocate General took a negative position regarding the right to be forgotten within the framework of the Data Protection Directive. Nonetheless, in the final judgment of 13 May 2014, the CJEU ruled that the Data Protection Directive does include the right to be forgotten.

Contrary to the opinion of the Advocate General, the CJEU ruled that the Data Protection Directive guarantees the right to be forgotten. In the reasoning of the judgment, the CJEU clarified the interpretation of the Directive on several key points. For example, the nature of a search engine, the territorial scope of the Data Protection Directive, and the responsibility of the search engine provider.

[6]As to this judgement, see Kranenborg (2015), Oro Martinez (2015).

This judgment is pioneering in recognizing the right to be forgotten and this tendency of the EU has had a great impact on the rest of the world in accelerating the discussion on the right.[7]

In the following sections, I will first identify the rationale of the new right and further clarify its meaning and scope.

2.2 Rationale

Why can a person seek the deletion of information concerning herself? It starts from the protection of personal data, based on the respect of the individual.

Information concerning an individual is traditionally covered by the right to privacy. The concept of privacy was born in the nineteenth century. Originally, it was understood as the "right to be let alone."[8]

The concept was developed in the middle of the twentieth century with four categories: (1) intrusion upon the plaintiff's seclusion or solitude; (2) public disclosure of embarrassing private facts about the plaintiff; (3) publicity which places the plaintiff in a false light in the public eye; and (4) appropriation, for the defendant's advantage, of the plaintiff's name or likeness.[9] This classification scheme is adopted in the Second Restatement of Torts.

Thereafter, with the development of computer technology, the concept of privacy has been further developed to reach the present version, "the right to control one's own information."[10]

The right to be forgotten is seen as an extension of this right. That is to say, in encountering a new phase of the information society, the concept of privacy has acquired a new face. Information spread in the world of the Internet can be deleted, because information is *under the control* of the data subject. It is also possible to explain that the right derives from the fundamental right of self-determination. In Europe, the right to be forgotten is supported by Article 8 of the Charter of Fundamental Rights of the European Union (2000/C 364/01), which provides "the protection of personal data concerning him or her." This also connects with Article 8 of the European Convention on Human Rights (ECHR), which provides for the respect for the private and family life without any interference, except in limited cases, such as national security or public safety.

---

[7]In addition to already mentioned Articles, see, e.g., Van Alsenoy and Koekkoek (2015), pp. 105 et seq., Marino (2014), pp. 1300 et seq., Hardy (2014), pp. 879 et seq., Picod (2014), p. 1068, Kranenborg (2015), pp. 70 et seq.

[8]Warren and Brandeis (1890), p. 195.

[9]Prosser (1960), p. 389.

[10]For example, Fried (1968), p. 482 ("Privacy is not simply an absence of information about us in the minds of others; rather *it is the control we have over information about ourselves*") [emphasis added]. See also Westin (1967), p. 5, Miller (1971), p. 25.

According to this idea, a person can withdraw information from the public eye as she decides and that decision should be respected by those in control of the information.[11] This is why the information, of which the deletion is sought based on the right to be forgotten, varies from case to case. It can be a picture of a party (as in the "drunken pirate" case, for instance), an article about property put up for auction (as in the CJEU González case), or information on previous gang membership of (as in the Tokyo District Court case of 9 October 2014, the very first case in Japan recognizing the right to be forgotten). Any, and all, such information belongs to the person, and that person can decide its treatment including the withdrawal from the public through deletion from the Internet.

It should be emphasized that, in essence, the right to be forgotten guarantees *the control over personal information* based on the idea that *it is considered as one of the fundamental rights*,[12] namely privacy.

2.3 Reactions to the Right to Be Forgotten

As mentioned above, the European Union has been a guardian of the right to be forgotten, as well as a pioneer in developing the meaning and scope of this right. In contrast, the United States has not been as supportive of the right to be forgotten.

Indeed, a parallel tendency with the EU can be found in the United States. Some states have adopted laws that admit the right to delete information published online. The most famous example is the Online Eraser Law of the State of California.[13] Moreover, in 2015, the White House accepted the Consumer Privacy Bill of Rights Act,[14] which also reflects contemporary understandings of privacy. This Bill is based on the principles of transparency, individual control, respect for context, focused collection and responsible use, security, access and accuracy, and accountability. To be emphasized here is the principle of individual control. Section 102, which provides for this principle, allows people to "make decisions"

[11]Cf. also the discussion around the "Privacy by Design (PbD)," concept proposed in 1990s by Ann Cavoukian, Information and Privacy Commissioner for Ontario. See, e.g., Rubinstein (2011), pp. 1409 et seq.

[12]The judgment of the CJEU also pointed out that the object of legislation concerning "the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognised both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law" (para. 3 10).

[13]A Chapter concerning the online privacy of minors (Chap. 22.1, beginning with section 22580) is inserted into the Californian Business and Professions Code. About the detail of this amendment, see http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB568. Accessed 21 September 2016. See also Lee (2015), pp. 1173 et seq.

[14]White House, Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015, available at: https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf. Accessed 21 September 2016.

about their personal data. It can be pointed out that this "control" is supported by the idea of a fundamental right of self-determination.

However, there are numerous examples of a dissenting view regarding the right to be forgotten in the United States. After the proposal of the right in the EU, an extensive number of objections were expressed by US companies as well as US legal scholars.[15]

Maybe because Europe and the US are opposed to each other regarding this right, the attitude of other countries also remains inconclusive and the discussion is prolonged.[16] This lack of consensus is troubling and it is obviously necessary to reach a degree of harmonization regarding the protection of personal data in an information society.

Currently, Europe seems to lead the discussion regarding online privacy, including the right to be forgotten. "Whether you like it or not, the EU is setting the standards for privacy protection for the rest of the world."[17] And, even if we agree that harmonization is necessary, given the global character of the Internet, does harmonization mean that *the rest of the world* must adopt a European standard? The answer should not necessarily be "yes."[18]

The right to be forgotten is a good example. The question is, by its nature, cross-border. Taking this point into consideration, it seems desirable to develop and share a common understanding of the right to be forgotten. Without it, companies working online would face significant legal risks due to privacy violations. This represents a significant obstacle to the development of today's society.[19] To obtain

[15]See, e.g., Freicher (2011), Ryan (2011), Saunders (2011). About the reaction of the SNS companies, see, e.g., Fiveash (2011), Promchertchoo (2011) or Walsh (2011).

[16]In Japan, the courts have changed decisions several times. While the decision of the Tokyo District Court of 9 October 2014 and the decision of Saitama District Court of 22 December 2015 recognises the right to be forgotten, the decision of Tokyo High Court of 12 July 2016 shows negative to the right. In Canada, the understanding of the right is narrower than that of the EU. See Gupta (2013), Cavoukian and Wolf (2014). The Office of the Privacy Commissioner of Canada, however, points out the necessity of the analysis of the right to be forgotten "in the Canadian legal context." The Office of the Privacy Commissioner of Canada, The OPC Strategic Privacy Priorities 2015–2020: Mapping a course for greater protection, available at https://www.priv.gc.ca/media/2071/pp_2015_e.pdf. Accessed 21 September 2016. In Switzerland, there is a case in which a business person sued Wikipedia, Google and other newspaper and broadcasting companies to delete information about him. This is considered as a case concerning the right to be forgotten. The Federal Court has admitted only a few requested deletions for the reason that the majority of information publication is done for the purpose of press reports. About the judgement, see press release of the Federal Court of 18 June 2015, available at http://www.bger.ch/fr/press-news-5a_658_2014-t.pdf. Accessed 21 September 2016.

[17]Valles (2001).

[18]About the response of other countries to the privacy rules of the EU at the beginning of 2000s, principally to the Data Protection Directive, see Heisenberg (2005), pp. 101 et seq.

[19]According to the StatCounter.com, the worldwide top 5 share of search engines (from August 2015 to August 2016) is as follows: (1) Google 89.14%, (2) Bing 4.33%, (3) Yahoo 3.35%, (4) Baidu 0.74%, (5) YANDEX 0.53%. As seen here, the most part is American which may not share the European concept of privacy.

a solid understanding of the right to be forgotten, Sect. 3 will examine some of the controversies concerning this right.

3 Controversial Issues on the Right to Be Forgotten

As mentioned above, there are mixed reactions to the right to be forgotten. What is the root of these differences? In this section, I try to unpack this controversy.

3.1 To Be Forgotten Equals to Be Delisted?

The first question is whether a search engine company is an appropriate defendant for a case of this kind. To analyze this point, let's take a simple example: John Smith finds a picture in which he and his girlfriend Jane are relaxing in his room. That picture is taken by his neighbor Tom and uploaded to Tom's blog site. For some reason, the picture attracts attention and goes viral on the Web. Now, when John *Googles* his name, the picture is found on the first page of the search results.

Traditionally, the person who divulges the information hidden by another person is considered as the infringer of their privacy. Based on this, in the example described above, John sues Tom for privacy infringement.

In cases of the right to be forgotten, however, the defendant is not the person who initially *shared* the hidden information, but the search engine as typified by Google or Yahoo that disseminates the information. That is, John takes action against Google, not against Tom, and the remedy is the deletion of the picture from its search results.

The point is that search engines are not the perpetrator in the publication of the information. This is the key feature of this "new" right. The focus here is that, even though Google accepted John's claim and deleted the picture from the search results, the picture remains in Tom's blog until John sues Tom directly (or the administrator of the blog).

As shown in even a simple example, in the information society of the twenty first century, the question of privacy has taken on a different character. It is not only a question of countervailing the power of those who reveal the information, but also of those who "list" the information.

The reasons for this are as follows: First, search engines are now the crucial gateway to accessing information. Second, the "listing" of the information is quite important (sometimes more than the actual information itself).

For the first point, when seeking information online the starting point is usually through a search engine.[20] With a few keywords and clicking the "search" button, it

[20]For the reference, Purcell et al. (2012).

is possible to easily find websites, which may include the sought information. The URL of websites becomes of secondary importance.

Search engines facilitate the finding of information, on the one hand, and have become one of the indispensable amenities of the information age. It can be said that search engines are a social infrastructure. We can no longer imagine a world without search engines.

On the other hand, however, search engines can reveal information, which might otherwise be unknown. In the past, before the popularization of the Internet, getting information was not straightforward because information was scattered widely and there was no easy way to find information. To find information, people needed to read newspapers, watch the news on TV or listen to the radio, find witnesses or go to a library. The sporadic character of information enabled information to remain out of the public eye.

This situation has changed dramatically with the development of the Internet. A mere search and a click reveals everything. Hard and meticulous effort is no longer necessary. We can find easily find by ourselves information that was previously difficult to find.

This relates to the second point, namely lists of information. Thanks to, or maybe because of, search engines, scattered information is now collected, compiled and listed up. Crucially, this change enables *profiling*. It is now possible to find intimate personal details of a person simply by googling her name. And, to some degree, we live in a world where "*You Are What Google Says You Are.*"[21]

It used to be harder work to establish facts because fact-finding required the collection and assemblage of fragments of information. These fragments then needed to be put together, much like a jigsaw puzzle. Smaller fragments would sometimes be missed out. With an online list provided by a search engine, however, we can now find information that would have otherwise been passed over. Even though each piece of information may be a mere fragment, it can combine with other information that can reveal other information that the data subject does not wish to make public.[22]

In an era of Big Data, profiling is much easier than before because the collection and combining of fragments of information becomes almost effortless. Now it can be said that profiling leads to a more scientifically reliable consequence because of the quality and quantity of materials of analysis, that is, information. Why? Because today the collection of information is automatic and the quantity of collected information is larger.

When information was collected manually, some information was inevitably missed by the data collector. In other words, information that the collector found unrelated, worthless or otherwise unnecessary was not the target of collection.

[21]Angelo (2009).

[22]Here, we can recall, for example, the question of the borrowing record of a library and privacy. Seeing the record, we can guess the borrower's interests, tastes or thoughts. Therefore, it is traditionally considered that the borrowing record should not be open to public without strong justification because this information falls within the scope of privacy protection. See, e.g., Miller (2009), pp. 19 et seq., Robertson (2011), pp. 307 et seq.

Moreover, some information may simply have been unintentionally left out. In this context, the unforeseen consequences for the data collector were neglected.

Today, however, such subjective decision-making does not disturb the act of investigative profiling. Information is *systematically* collected and its combination can reveal unanticipated facts. For example, the purchase of unscented lotions or soaps, or of supplements of calcium, magnesium and zinc, may indirectly reveal the fact of pregnancy.[23] Information becomes a resource to reach highly personal conclusions about a person's health, state of mind and so forth.[24]

In this respect, removing information from a list has great significance. This is because the aggregation of information has important consequences. Information that in isolation has no special significance can, when combined, shed light on other information that may be more important or otherwise hidden. Therefore, it is of great interest to be *delisted* from search engines, even if the information itself does not vanish from the website where it is hosted.

As mentioned, search engines play a major role in an information society and their "results" can sometimes cause a breach of privacy, even though it is not the search engine that reveals the information in question.

It should be stressed that a consensus on this point has not been reached. As already noted, the CJEU has held them to be a "data controller" and they have a certain responsibility on the treatment of information.[25] However, some argue that search engines are mere intermediaries and search results are not a breach of privacy because it is mechanically and randomly generated by algorithms. Based on this thought, the claim to delete information from the search results should not be admitted.[26]

As just described, the defendability of search engines is a complex question. Given the fact of search engines, however, it is not impossible to require search engines to delete information from the search result list. This should be justified because search engines offer a means to access, as well as widely transmit, information. In terms of the accessibility to information, the "delisting" from a search engine is weightier than the deletion of the information itself from a certain website, because people, except those who already know the URL, lose the possibility to access that site.

---

[23]Duhiggfeb (2012).

[24]Article 22 of the Data Protection Regulation of the EU provides the rights of the data subject concerning the automated individual decision-making, including profiling.

[25]See the above-mentioned CJEU judgement of 13 May 2014 (C-131/12). Because of its importance to society, the liability can be justified. See Jones (2014), p. 599.

[26]In Japan, for example, the attitude of courts is not consistent. Some court decisions have ordered the deletion of information. For example, the decision of Tokyo District Court of 9 October 2014 or the decision of Saitama District Court of 22 December 2015 (the court decides that the search result is "edited" according to the policy of the search engine even though the collection of information is mechanical). Other courts do not recognize the liability of search engines, for example the decision of Kyoto District Court of 7 August 2014 (saying that the URL as well as the snippet are mechanically and automatically acquired from the website and the search engine does not show the fact itself). About the discussion in Europe regarding this point (specifically in the UK), see Hurst (2015), spec. pp. 188–193.

3.2 Antagonistic Interests

However, it is not adequate to admit such deletion (or the delisting) without any restriction. The right to be forgotten should not be absolute and it is at the same time essential to guarantee other interests. The primary competing interests which should be taken into consideration here are the right to know and the freedom of expression.

The range of information which can be deleted based on the right to be forgotten is wide. Not only information that the data subject has published by herself, but also "any information relating to a data subject."[27] This definition seems to cover any type or kind of information about that person. As previously mentioned, even petty information can provide an important clue in establishing more important information.

There is no doubt that the respect of the individual is one of our fundamental values and that nobody's life should be disturbed. It is for this reason that we should have the right to control information concerning ourselves.

This does not mean, however, that everyone can freely erase information or personal data. If all information could be erased, what would happen? People would want to delete all inconvenient information from the web, even if there are important justifications for such information being available to society. Large-scale erasure of data would severely inhibit access to information and the right to know.

A typical hypothetical example might go as follows. A politician accepted bribes 45 years ago. It was when she was still young and not yet accustomed to the manners and risks of the world of politics. Realizing that her act was inappropriate, she returned the money to the giver. She received a strong censure from her party, but was not subjected to any legal sanction. She never repeated such action from then on; it was a single mistake in a long and distinguished career. However, she notices that the news of this isolated case of accepting a bribe continues to show up in the search results when she *Google*s her name. She fears that it might threaten her career and she asks for the deletion of this information from the result list.

Should this claim be admitted? The answer to this is almost certainly no. The information of the acceptance of bribes by a politician—even if it was decades ago and an aberration—is of on-going importance for voters because corruptibility can be one of the deciding elements in making a political choice.

The right to be forgotten is problematic precisely because it can be an excuse to *rewrite* the past. Information which should be known to the public cannot be deleted or shut out solely for the reason that the information is disadvantageous to someone Access to information is the basis of a democracy. The right to know is one of the fundamental rights of political modernity.[28]

In this respect, the right to be forgotten and the right to know are two sides of the same coin. If the importance is put only on one side of the right to be forgotten, people lose the possibility of access to that information. As mentioned above,

[27]Rosen (2012a).

[28]See also Article 19 of the Universal Declaration of Human Rights of the United Nations.

search engines are now the "front door" to gathering information on almost every topic. Considering this crucial role, arbitrary claims based on the right to be forgotten should be avoided or, at least, treated with the utmost caution.

Some information falls within the range of the public interest and should be open to the public even though it represents an embarrassing truth for someone.[29] The words and deeds of a public persona, as mentioned in the example above, by their nature should be made public. For reasons of public security, crime records can also be deemed so.[30] Such information should be known to the public to maintain the society and the life of people and its disclosure should be guaranteed.[31]

To go further, shutting out of access to information can also inhibit the development of society. The International Federation of Library Associations and Institutions (IFLA) has expressed concern on the possible limitation of access to information by the right to be forgotten.[32] Being aware of the importance of the protection of privacy, on one hand, the IFLA states, on the other hand, that "the ideal of freedom of access to information cannot be honored where information is removed from availability or is destroyed."[33] The IFLA stresses the necessity of the preservation of information for some purposes (historical, statistical, biographical, genealogical and other research). The EU is also conscious of this point and Paragraph 3 of the Article 17 of the Data Protection Regulation provides an exception of the right to be forgotten. According to this provision, data necessary for the archiving for the public interest, for the scientific or historical research or for the statistics should not be erased (item d). The problem is, as the IFLA worries,[34] there is no solid criterion to identify such information.

Moreover, the accessibility to information reminds us of the problem of censorship. As access to information is the basis of the fundamental right to know, the interruption of the flow of information should be treated with caution.

---

[29]Freicher (2011).

[30]The right to be forgotten is originally proposed "historically…in exceptional cases involving an individual who has served a criminal sentence and wishes to no longer be associated with the criminal actions." Ambrose and Ausloos (2013), pp. 1–2. Often the exposure of the criminal record is questioned in relation to the privacy. Some cases concerning the right to be forgotten are also on the criminal record (for example the decision of Saitama District Court of 22 December 2015).

[31]The above-mentioned CJEU Judgement has also referred to this point (para. 97 explains that the deletion is not admitted "if [the data subject's name] appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of inclusion in the list of results, access to the information in question.").

[32]IFLA Statement on the Right to be Forgotten (2016), 31 March 2016, available at http://www.ifla.org/publications/node/10320. Accessed 28 September 2016.

[33]IFLA Statement on the Right to be Forgotten (2016).

[34]IFLA Statement on the Right to be Forgotten (2016) ("When search engines make the decisions, their full consideration of the issues of privacy versus the public interest is not transparent.").

In the thirteen months after the landmark CJEU judgment of 13 May 2014, Google received close to 270,000 requests of deletion of information and accommodated more than 40% of these requests.[35]

What should be highlighted here is the fact that Google decides on whether the link should be deleted or not. Is this appropriate? Would it be more appropriate to delegate such a decision to the private sector?

It cannot be denied that there is a risk of an arbitrary ruling.[36] At the same time, the extension of the right to be forgotten causes worries of an excessive voluntary restraint on the part of search engines. They might be hesitant to put some information in their research list for fear of being sued for breach of privacy. This leads to the situation that people can access less information, because we lose the opportunity to find it.

The decision to delete the link is of the nature of the selector of information, which should be known to the public. It should therefore be done after cautious scrutiny, otherwise the public interest, the right to know, cannot be guaranteed. Even though search engines have already become a crucial social infrastructure, it is surely too much that they are also delegated the task of making such difficult and potentially controversial judgments. At the same time, it should not be adequate to entrust this decision to the government because the accessibility to information (and the right to know as its basis) is one of the core axes of any democracy. We can easily enumerate examples in history wherein a government tried to control people and the society by information control.

It is a delicate issue and we cannot readily reach the answer.[37] In this sense, the actual situation remains rather fragile.

Furthermore, the right to be forgotten is often singled out for criticism in relation to the freedom of expression. One of the reasons is somewhat indirect. For democracy, the freedom of expression is essential. To have free speech, people should have access to all information necessary to consider and make informed

[35]Guiton (2015).

[36]Of course, search engines release their policies on the removal of search results to guarantee the transparency, but it is the search engines that have the final say. This concern is expressed also by the NGO Reporters without Borders (RWB). The RWB describes the CJEU judgement of 28 May 2014 as "opening Pandora's box which would be difficult to re-close" and the situation where search engines are delegated to decide to delete the information as an "infernal spiral." RWT, L'engrenage infernal du droit à l'oubli, 4 juillet 2014, available at https://rsf.org/fr/actualites/lengrenage-infernal-du-droit-loubli. Accessed 30 September 2016.

[37]The above-mentioned NGO, RWB, insists that the decision should be done by the courts. See Recommendations on the Right to Be Forgotten by La Quadrature du Net and Reporters Without Borders, 26 September 2014 ("Responsibility for a decision involving individual freedoms that should be handled by a court is thereby delegated in practice to a private sector company. This delegation of responsibility is all the more dangerous because the ruling is based on vague and general principles that provide no guarantee for freedom of expression."). Available at https://rsf.org/en/news/recommendations-right-be-forgotten-la-quadrature-du-net-and-reporters-without-borders. Accessed 30 September 2016.

judgment. As the right to be forgotten puts the limit to the access to information, it threatens also the freedom of expression as a consequence.

The other is the pressure to facilitate expression. If the right to be forgotten is widely recognized and information can be deleted, people may get demotivated and intimidated to put other information on the Internet.[38] This will have a dramatic effect, suppressing the free flow of ideas and discourse needed in an open society.

3.3 Privacy Knots

The right to be forgotten is a newly-proposed concept in the twenty first century, but it sheds light on the fundamental and traditional questions on privacy. It should be stressed here that it is time to re-examine the privacy in response to such changes.

In the question of the right to be forgotten, some interests are in conflict and it is necessary to find the right balance. However, before considering how to balance these interests, we should comprehend some fundamental issues concerning privacy.

First, regional differences in the understanding of the privacy should be underlined. On this point, differences are found between Europe and the United States. Both consider it as a fundamental right, but the content and scope of the right is not the same.

As is well known, the modern concept of "privacy" originated in the famous article by Warren and Brandeis at the end of the nineteenth century. As already mentioned, the idea was developed in the United States by Prosser or Westin in the 1960s to refer to the right to control information about oneself. In Europe, on the other hand, the interests covered by the privacy in the United States are protected by, for example, the French right to private life (droit à la vie privée) or the German right to informational self-determination (informationelle Selbstbestimmung).

The root of this difference is found in the basic legal values of dignity and liberty.[39] When talking about privacy, Europeans put the emphasis on the respect of the individual and personal dignity, while the American discussion emphasizes liberty from state interference. This difference, roughly speaking between civil law and common law, should be taken into consideration when examining the right to be forgotten.

Based on the European idea, nobody should be able to damage the "social image" of others.[40] The right of privacy is, in other words, the right to object to any actions that injure personhood within society. Based on this idea, a conflict concerning privacy is rather horizontal. The defendant is mostly a private person, including, in many cases, the media.

---

[38]See Rosen (2012b), p. 1533.

[39]Beignier (1992), pp. 60–61, Whitman (2004), pp. 1160–1164.

[40]Whitman (2004), pp. 1164 et seq.

In contrast, according to the American understanding of privacy, the potential enemy is usually thought of as the state. The core of the privacy right is to be free from state interference, specifically in the private sphere.[41] This is why privacy rights are often discussed in the context of the First Amendment, which guarantees the free speech and freedom of press.[42]

This difference ties in with the abovementioned differing reactions to the right to be forgotten. Europe gives more weight to the dignity of the individual, including privacy. The right to be forgotten should be widely admitted because it is one of the necessary tools for ensuring this goal. On the contrary, according to American thought, free speech is more important because it is a way to defend ourselves from arbitrary governmental interference. As the right to be forgotten is often claimed against private actors, it is somewhat distinct from the understanding of privacy and, therefore, it can be more difficult to accept this right.

As already noted before, the right to be forgotten is cross-border and international by its nature. It is not enough nor meaningful that each country or legislation expresses the pros and cons of this new right. It is needed to find a balancing point of values within global standards. This discussion is on-going and it will take time to reach a resolution. It is necessary to return to the fundamental issues on privacy and the surrounding values.

Additionally, to consider the right to be forgotten and privacy, the question of consent should also be highlighted. In a Japanese case on the right to be forgotten (the decision of Tokyo District Court of 1 December 2015), the parties had a discussion on whether consent was given.

Briefly, the plaintiff, a Japanese national, sued Google Inc., seeking to delete 237 search results with his name, claiming that the titles and snippets of the search results included disadvantageous information for him. The information was about the fact that he was a member of a delinquent group in his youth (the plaintiff could not obtain bank loans because such information could easily be found on the Internet). The point of contention was that the plaintiff had once talked openly about his past on a TV program. The defendant, *Google Inc*., claimed that since the plaintiff openly disclosed the information about himself, he had consented to waive his privacy right.

Assuming that this claim is acceptable, does the disclosure of the information also mean consent to keep that information in the public domain indefinitely after its publication? Is it then enough that search engines (and other Internet sectors) prepare the terms of use including the provision of a consent clause on privacy, claiming that the published information is in the public domain and not in the private domain?

---

[41]Whitman (2004), p. 1161.

[42]The First Amendment states that the federal "Congress shall make no law…abridging the freedom of speech," which is also applied to state governments [cf. Gitlow v. New York, 268 U.S. 652 (1925)]. The balance between these two values, which has been long discussed, remains contemporary; recently some point out the "privacy restriction" of the First Amendment. See, e.g., Volokh (2000), pp. 1050 et seq., Richards (2005), pp. 1149 et seq., Fazlioglu (2013) pp. 155–156.

As previously mentioned, the initial concept of privacy is the right to be left alone, and has, over time, transformed into a right to control information about oneself.[43] It is now considered as a part of the right to self-determination. If so, it seems to be possible for the data subject to freely decide the treatment of information, including disposition by consent. Since the 1960s when the concept of privacy has been developing, the importance of consent in the context of the privacy is often pointed out.[44]

The right to be forgotten has a similar background.[45] The Data Protection Regulation assumes the existence of the consent for data processing (Article 7), and the right to be forgotten allows the withdrawal of this consent. This should provide a basis for the idea of privacy as the control of the information and the right to self-determination. The withdrawal of consent is also in the framework of control, according to this perspective.

However, some points should be questioned. First, there is the validity of the consent. Based on the principle of information control, some have no doubt on the consent of privacy. However, others do not agree with this concept of "privacy self-management."[46] They argue that control of information in today's world with the Internet is purely theoretical. Nowadays, huge volumes of information are constantly being processed everywhere online. Realistically, no one can know the entire processing of personal information on the Internet. In addition, the practice in information society is that only one click of an "agree" button shows consent and very few people ever read attentively the terms of use.[47] Should it be considered as genuine consent? It seems that it has become a mere formality today. With such "empty" consent, is it possible to say that people have control over their information? This creates the risk of providing an excuse to the data collector that their action is legal.[48]

Even though one expresses her consent on privacy once and the consent is perfectly genuine at that time, she can legitimately change her mind later on. If it is accepted that this acceptance can always be changed, it is tough for the data collector to deal with any information. To take the consent as absolute, on the other hand, the fundamental value of the data subject may be damaged. Considering so, the consent theory has its limits.

To go further, considering that the privacy is one of the fundamental rights, is it possible to admit completely its disposition by the consent of the individual? Let's go back to the abovementioned Japanese case. Does mentioning a piece of personal

[43]Westin (1967), p. 5 explains the privacy as the right to "determine…when, how, and to what extent information…is communicated to others."

[44]Westin (1967), p. 420.

[45]Ausloos (2012), p. 147.

[46]Solove (2012), pp. 1880 et seq.

[47]Morrison (2015).

[48]Solove (2012), p. 1881.

information in a TV program constitute consent to waiving privacy? Is it possible, more fundamentally, to waive the right of privacy, at all?

In civil law countries, including Japan, privacy is one of the rights of personality and it has constitutional value and protection. Considering this point, the contract which requires the waiver of such rights can conflict with public policy. It seems that many of the actually-used terms of use, which includes the provision on the consent on privacy, neglect to consider this point.

Indeed, little conflict is so far realized. However, as the actual position of privacy remains fuzzy and this can destabilize the information society itself. It is therefore an urgent issue to reconstruct the concept and theory of privacy in an information society.

4 Next Phases and Challenges

The previous section has tried to layout the whole context and the related issue of the right to be forgotten.

The primary question on this right is the relation between privacy and the right to be forgotten. Is the right to be forgotten a part of privacy, does it partly overlap, or is it a totally different right? The answer is the former, that is to say, the right to be forgotten can be considered as an extension of privacy. However, it has some differences from the traditional privacy concept and it is not surprising that the right is sometimes explained as a "new" right. The characteristics of the right to be forgotten originated from the attributes of the new form of the society, the information society.

As the right is an extension of privacy, it should be covered by the general theory of privacy. However, because of the differences, some modifications should be considered. Because of the short analysis, the concept of the right to be forgotten still remains unclear. The last section will point out the next questions to be analyzed to configure the right to be forgotten.

4.1 Resetting Privacy Criteria

On the Internet, there is a great variety of information. Some should be forgotten; others should be remembered. Of great importance is where we draw this line.

In the traditional theory of privacy, some standards for what information should be covered by privacy are set. Although the detail differs according to legislation, we could find the common denominator. The boundary is whether the publication of the information is in the public interest. If the information in question is in the public interest, even though it is in the private field, the information should be open to the public. A classic example is a criminal record. If the data subject is a public

figure, information relating to her should be the object of public concern and it should be divulged.

The point to be considered here is the social change. As repeated in this chapter, in contemporary society, information technology has developed. Considering these circumstances, is there no problem to use the same criteria as before? More precisely, it should be necessary to take the characteristics of the Internet itself into consideration. First, "*the Internet doesn't forget.*"[49] Second, the Internet is a "raker" of information.

Having these characteristics, what is different from before? Today, it is much easier to dig up the past. Before, with the elapse of the time, information "weathered." New information piled up on older information. To find old information became ever more time-consuming and costly and little by little it disappeared from public memory. However, the Internet keeps information theoretically for eternity.[50] Any information can appear with the mere click of the search button.

Additional to this, the Internet, specifically search engines, lists up various other information. As mentioned in the previous section, this list of fragmented information may enable us to infer facts that someone would rather not disclose.

In short, it is more difficult to hide information and make a break with the past. Oblivion is a form of forgiveness.[51] If the Internet delivers the *end of forgetting*,[52] we are always held captive by the past. Errors of the past deprive us the possibility of change.[53] It is undesirable because it should disturb the chance for betterment of individuals and, as a consequence, the advancement of society.

The importance of rehabilitation is also focused in the traditional theory of privacy.[54] Although the lapse of time was one of the most important factors, in a society with the Internet, it loses its meaning. Today therefore, the criteria of privacy should be the possibility of a reset and be reconfigured to adjust to such a society.

4.2 Divergence on Balancing Values

The last question is *who* should decide. As previously pointed out, the balancing of values differs from one piece of legislation to another. In the evaluation of privacy, one puts importance on the dignity of the individual whereas the other considers the

[49]Ausloos (2012), p. 143.

[50]Ambrose (2013), pp. 11 et seq., points out the temporality of information on the web. A good deal of information disappears soon and it is not necessarily saved for all time.

[51]Bennett (2012), p. 167.

[52]Rosen (2010).

[53]Solove (2006), p. 531 ("People grow and change, and disclosures of information from their past can inhibit their ability to reform their behavior, to have a second chance, or to alter their life's direction.").

[54]Bennett (2012), p. 170, citing Melvin v. Reid [297 P.91 (Cal. Ct. App. 1931)] and Briscoe v. Reader's Digest Association Inc. [483 P.2d 34 (Cal. 1971)].

right to know as more important. Assessing the lapse of the time should also be different. All of this leads to the different reactions regarding the right to be forgotten.

The judging court should be critical. If González brings a case to the Spanish (or other European) court, his claim will be admitted, while he may not succeed in an American or Japanese court.

In addition, the applicable law will also be in question. When a case has an international dimension, Private International Law (PIL) should be taken into consideration. The PIL is the rule to choose applicable law(s), law(s), which then governs the case. Using the PIL rules, the court designates the applicable law, which can be not only law of the forum but also a foreign law. It is then possible for González to bring a case to the Japanese court and the court applies Spanish law.

However, the designated applicable law can be overridden by the law of the forum to protect the public order of the forum. As noted above, several fundamental values are in question in the context of the right to be forgotten, extended privacy. The protection of the fundamental rights is in the framework of public order, and the court can exclude the application of foreign law(s).

Because American companies form the majority of the more frequently-used search engines, cases on the right to be forgotten often have an international element.[55] For example, González sued Google.com, an American company. In Japan as well, the plaintiffs sued Google.com or Yahoo.com, not Google Japan or Yahoo Japan.

It is therefore indispensable to analyze the PIL question, but this discussion—thus far—remains immature.[56] The CJEU (and also Japanese courts) have ignored the analysis on the PIL question in their decisions. This results from the instability of the right to be forgotten concept itself.

The first need is therefore to modify and reconstruct the concept of privacy, to adapt to the information society. And then, the reconciliation among countries with different values should also be considered.

[55]As already mentioned, the market of search engine is controlled by American companies, and on the other hand the plaintiff is often non-American, in many cases European. A difference in the sense of privacy is pointed out: "Americans want to be famous while the French want to be forgotten." Rosen (2012b), p. 1533.

[56]The EU is aware of the question and it has published the opinion on this issue (Opinion 8/2010 on applicable law, adopted on 16 December 2010. Available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_en.pdf. Accessed 7 October 2016). However, as it is the discussion in the framework of the Data Protection Directive and the Data Protection Regulation will be soon in force, the discussion should be renewed and more developed.

5 Current Situation Regarding the Right to Be Forgotten in Japan

This section tries to describe the actual situation of the right to be forgotten in Japan. As already mentioned, the concept was born and developed mainly in Western countries. It should, however, be interesting and useful work to analyze the reception of this "newly born right" in other parts of the world.

5.1 A Protero-Right to Be Forgotten

With the development of Internet technology, in Japan the number of cases claiming the deletion of information published online has been growing. In the first stage, the majority of cases were claims seeking an injunction against publishers of journal or newspaper articles on the grounds of defamation or the infringement of privacy.

Since around 2008, cases against search engines started to appear.[57] The reason for this tendency to sue search engines is to obtain an effective and efficient result. In Japan, the existence of anonymous "textboards," represented by 2channel,[58] and also the outspread of various curation sites,[59] facilitate the infringement of the legal interests of others. As it is quite normal for these textboards to put their servers abroad, as the controller of such curation sites is unknown and as the information in question spreads quickly, it is often costly and time-consuming for a victim to ask for the deletion of a problematic post. Hence, the victims have tended to sue search engines, rather than the "provider" of the information.

Moreover, there are some varieties regarding the object of litigation.[60] The simplest type of litigation is to seek the deletion of the infringing material. This kind of claim is directed mainly to the controller of websites or textboards. As mentioned, however, this is not realistic.

Therefore, a second option for the plaintiff is to ask search engines to delete the material from the list of the search results. In the results list, users can find a snippet of information and a link to the problematic website. With the deletion of the information from the results list, the public loses the opportunity to access the information, and then it is almost the same as if the information is hidden from the public eye.

---

[57]Sogabe (2016), p. 4. A decision of a district-level court is found (decision of the Tokyo District Court of 14 November 2008).

[58]The most famous anonymous textboard in Japan, launched in 1999. In such anonymous textboards, many infringing writes can be found.

[59]Called in Japanese language "*matome* [meaning "compilation"] site"; it designates a round-up and add-up site which collects and "copy-and-pastes" information from other websites, SNS or anonymous textboards,.

[60]As to the variation of cases in Japan, see Mori (2015), pp. 51 et seq.

Furthermore, there are cases that claim that the combination of some words infringes the honor and reputation of the plaintiff. Many search engines offer the function of "suggestion."[61] When users input a key-word in the query, this function "suggests" other key-words, which are related with the former. If a person inputs his name in the search box, for example, and the function "suggests" a key-word such as "murder," then users could be given the impression that the person commits, or at least has a relationship with, the crime. It is then possible that the person claims that this "suggestion" is defamatory.

In Japan, the question of *who* should be the defendant is actively questioned. The defendant in many cases is the enterprise providing the search engine service, but it is not the "perpetrator" of the publication or the distribution of the information. It should not be appropriate to force search engines to be the defendant only for the reason of the effectivity and the efficiency of the plaintiff. In fact, the search engines claim to be a mere vehicle or mediator of information communication.

In Japan, the information mediator should bear a share of the responsibility. The Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers and the Right to Demand Disclosure of Identification Information of the Senders (hereinafter the "Providers' Liability Act") has a special provision regarding the general rule of torts (Article 709 of the Japanese Civil Code) concerning the civil liability for damages of the Internet service provider. Originally, this Act aimed to limit the responsibility of the information mediator because they are not the addresser of the information. However, Article 2, Paragraph 3 of the Providers' Liability Act does not include the search engine in the list of the service provider.[62] This Act, therefore, is not directly applied to cases against search engines.

Although the Providers' Liability Act does not suppose the search engines as its target, considering their characteristics and roles to facilitate the communication of information, it seems that they are deemed as the service provider provided by the Article 2 of the Act.[63] Considering the fact that many judgments and decisions of the lower-level courts admit that the search engine should be the defendant, it can be pointed out that the stance of the Japanese courts is that the search engine is liable for the defamation or the infringement of privacy arising out of the publication and distribution of information.[64]

---

[61]For example, the decision of the Tokyo District Court of 19 March 2012. See also Ogura (2013), pp. 22–23.

[62]Article 2 (3) defines the "telecommunications service provider" as "a person who relays others' communications with the use of specified telecommunications facilities, or provides specified telecommunications facilities to be used for others' communications."

[63]Sogabe (2016), p. 9.

[64]See, e.g., the judgement of the Tokyo High Court of 12 July 2016 admitting that "the claim of the defendant [search engine] of not being liable for the defamation because of being a mere information mediator cannot be accepted." Of course, the liability of the search engine as information mediator is different from that of the information addresser. The former is limited and admitted more narrowly than the latter. On this point, see Mori (2015), pp. 53–54. See also Ogura (2013), p. 23. Some scholars oppose this stance of the courts. See Matsui (2013), p. 401.

Turning to the more theoretical point, in cases claiming the deletion of information, the legal basis of the plaintiff's claim is the defamation or the infringement of privacy. Before the case of the Tokyo District Court of 9 October 2014, the term "right to be forgotten" had never been used.

Regarding defamation and the infringement of privacy, these two categories of right have been well-theorized in Japan. Therefore, such contemporary claims concerning information on the web are treated within existing theory. Both defamation and the infringement of privacy are considered in Japan as the infringement of the right of personality. These interests are deemed as the right to be legally protected (Article 709 of the Japanese Civil Code) and those for whom the right is infringed can claim an injunction to stop the alleged infringing acts, as well as compensation. Deleting the search results is one of the injunctions standing on the infringement of the right of personality.

Firstly, the criteria of defamation and the infringement of privacy have been established by decisions in earlier cases. As to the defamation, the first leading case is the judgment of the Supreme Court of 11 June 1986, admitting a prior injunction of a publication based on the infringement of honor and reputation. Granting of the injunction was conditional on the injunction not discouraging freedom of expression. To balance freedom of expression and protection of the right of personality, the Supreme Court set as the criteria the principle of "pubic interest" and of the "truthfulness" of the expression in question. In the context of the principle of the truthfulness, it is enough that the actor misidentifies that the fact is true and has an adequate cause to do so (the judgment of the Supreme Court of 25 June 1969).[65]

Interestingly, the judgment of the Supreme Court of 15 March 2010 has referred to the understanding of this principle in the context of expressions on the Internet. Although the preceding judgment of the lower-level court in this case ruled that the principle of the truthfulness should be mitigated, because of the difficulty for individual users to confirm what is the truth (the judgment of the Tokyo District Court of 29 February 2008), the Supreme Court adjudicated that the principle should also apply information published on the Internet.

In addition, the infringing expression can be also restrained if the damage to the victim is greater than the interest to be protected of the author of the expression and also the public interest to know (the judgment of the Supreme Court of 8 February 1994; the judgment of the Supreme Court of 24 September 2002).

The criteria for the infringement of privacy are shown in the leading case of the judgment of the Tokyo District Court of 28 September 1964: (1) the expression is true or seems true for the public (the *factualness*), (2) the data holder wants to hide the fact (the *confidentialness*) and (3) the fact remains unknown to the public (the *unknowingness*). As there are no decisions that modify these criteria in light of the

[65]It should be pointed out that the judgement of the Supreme Court of 25 June 1969 is a criminal case, but the criteria shown in this case seems to be taken in consideration in civil cases. See also Ogura (2013), pp. 20–22.

special characteristics of the Internet, these criteria also apply to the infringement of privacy online.

In Japan, therefore, the deletion of information in a claim against a search engine is judged within the framework of existing privacy theory and legal tests in Japan. There has been no example of a Japanese court referring to a right to be forgotten, prior to the CJEU judgment.

5.2 Decisions of District Courts

As previously mentioned, there are some examples of cases in which the deletion of information is sought against a search engine. The claims of the plaintiff, in such cases, have been based on the theory of the defamation or the infringement of privacy.

The earliest case published is the judgment of the Tokyo District Court of 18 February 2010. In this case, the plaintiff, a doctor, demanded the deletion of false information about himself on a textboard, claiming that the display of that information in the list of search results was defamatory. The Court ruled that the display was a mere abstract of other websites and there was no intention on the part of defendant, i.e., the search engine, and the display itself was not considered as a defamatory act. In brief, in the first phase of cases, claims against search engines were not admitted.

The CJEU judgment of 13 May 2014 had a great impact on this apparently stalled situation. The news about the CJEU judgment was widely broadcasted, also in Japan. And then, in the discussion in Japan, a wave of influence arriving from the EU can be found.

The term, the "right to be forgotten," was mentioned before the court for the first time in the proceedings of the decision of the Kyoto District Court of 7 August 2014. The allegation of the plaintiff claimed, referring to the CJEU judgment of 13 May 2014, as follows: "In May 2014, the CJEU ordered a company to delete links to websites which included information that the plaintiff does not wish others to know. In this case as well, the claim of the injunction should be admitted from the viewpoint of the protection of the honor and privacy of the individual, which originates from the right to the pursuit of happiness guaranteed by the Constitution."

However, the "new" concept of the right to be forgotten has not been easily accepted by Japanese courts. In the abovementioned case, the Kyoto District Court did not accept the claim of the plaintiff (moreover, the appeal court, in the judgment of the Osaka High Court of 18 February 2015, upheld the decision of the District Court).

The turning point was the already-mentioned decision of the Tokyo District Court of 9 October 2014. The court ordered, for the very first time in Japan, the deletion of the search result from a search engine. Although the term "right to be forgotten" itself did not appear in the text of the decision of the court, it is broadly

reported that it is the very first case in which a Japanese court recognized the new right. Many of the reports in the mass media referred to the CJEU judgment.

Looking at the decision of the Tokyo District Court, the structure of the reasoning to admit the deletion of the information from the search results is based on an infringement of privacy. The Court ruled that "the legal interest not to have information of criminal records published with no good reason is one of the rights of privacy." This expression seems to indicate that the court took a "traditional" approach.

It should be emphasized, however, that the CJEU judgment had an impact on the Japanese situation. Even though the term, the right to be forgotten, is not clearly cited in the documents of the parties or in the procedure, the attorney representing the plaintiff was clearly conscious of the CJEU decision.[66]

Possibly influenced by this decision, the Saitama District Court on 22 December 2015 admitted the claim of the plaintiff to delete information from a search engine. The Court held that "even though it depends on the nature of the crime, people have the "right to be forgotten" by the society regarding a crime committed in the past, after a certain period of time has passed."

The decision of the Saitama District Court did not explain the further details of the "new" right and its reticence triggered fierce argument in Japan. Even though the explanation of the court officer was published, the reason why the Court accepted the new concept remains unclear.

What should be pointed out here, however, is the simplification of the logical structure to claim the deletion of the information.[67] Based on the traditional theory of defamation or the infringement of privacy, the various requirements in the abovementioned leading cases needed to be established.

If the alleged victim takes the defamation approach, the information in question should be defamatory. It is not, however, necessarily defamatory information that will be in question in the claim to delete information from a search engine. Even though the information is purely positive and favorable for her, she might still want to hide the information.[68] As the question of what information should be hidden is often quite subjective, the defamation approach is sometimes not appropriate for the victim in a case involving the deletion of information from a search engine.

This is also the case when taking the privacy infringement approach. One of the three requirements, the factor of "*unknowingness*," is often in question. The information in the context of the right to be forgotten is quite often once-published and in the era of the Internet, such information—once-published—cannot

[66]See Kanda (2015), pp. 42–43.

[67]Kanda (2016), pp. 43 et seq. This article explains the logic from the viewpoint of the plaintiff.

[68]For example, interestingly, Japanese people hope to stay anonymous (or sometimes they use pseudonym) when they make a donation. Suppose a case that a person makes an anonymous donation and a newspaper publishes an article with his real name. This article should not be deemed defamatory because his reputation is not damaged.

disappear. In this situation, considering the factor of "*unknowingness*," it becomes difficult to ground a claim on the infringement of privacy.[69]

If it is possible to base the claim on the right to be forgotten, the plaintiff can be freed from the evidential challenge of proving defamation or an infringement of privacy. This would be one of the principal reasons for the increase in the number of cases in Japan involving the right to be forgotten.

5.3 Japanese Reaction

As seen above, the introduction of the concept of the right to be forgotten in Japan is quite strategic in cases involving the deletion of information against the search engines.

Japanese Courts, however, do not yet recognize the right to be forgotten. The appeal court decision of the case of the abovementioned Saitama District Court—the decision of the Tokyo High Court of July 12, 2016—clearly mentioned that "Japanese legislation is unaware of the existence of a so-called right to be forgotten" because "the requirements and the effect of this right remain unclear." The court considered "the substance" of the right to be forgotten as the "right to demand an injunction based on the right to honor or the right of privacy, one of the contents of the right of personality."[70]

However, as already mentioned in the previous section, the existing approaches are sometimes not enough to claim the deletion of information that is available on the Internet. This fact leads one to conclude that the new concept, the right to be forgotten, is a tool to combat against the diffusion of information on the Internet.[71] Even though it should follow the existing theories, the criteria are not clear because the conditions have been shown in the precedents decades ago and do not fit the actual situation of today's society.

Some of the cases concerning the right to be forgotten, of which the lower-level courts have already made the decision, are pending before the Supreme Court and a decision will be made soon. This will fix the stance of Japanese courts to the right to

[69]Kanda (2016), p. 44. In fact, in the cases of the Tokyo District Court of 9 October 2014 or of the Saitama District Court 22 December 2015, the defendants counter-claimed that the plaintiff's claim lacked the "unknowingness" factor because the information in question was already published and known to the public.

[70]After the completion of this chapter, the Supreme Court of Japan published a decision on this issue. The decision of the Supreme Court of 31 January 2017 (the final appeal decision of the case of the decision of the Tokyo High Court of 12 July 2016) ruled that the deletion of information should be dealt with in the framework of the existing theory of privacy, balancing between individual respect and public interest, without referring to the term "right to be forgotten."

[71]Although the majority of the scholars consider that the right to be forgotten is not necessary, as well as the opinion of the Japanese Court, some argue the necessity of law-making. See Miyashita (2016), p. 35.

be forgotten and is eagerly awaited. It is necessary to follow continuously the movement of the Court and also the academic discussion.

Waiting for the decision of the Supreme Court, governmental action should also be noted. The Ministry of Internal Affairs and Communications (MIC), whose mission is the regulation of telecommunication affairs, is also interested in the right to be forgotten. One of the committees of the MIC, ICT Service Safety and Security Study Group, has published the report on the 17 July 2015, titled "Response to Distribution of Personal Information and User Information on the Internet" (the Working Group Report).[72] The Working Group Report refers to the right to be forgotten, but limits itself to present the situation in the EU.

Throughout the Working Group Report, the MIC reveals a negative stance to the recognition of the right to be forgotten. The main reason for this seems to be the differences and diversity among countries in their understandings of privacy.[73] It should be noted that the MIC does not hope for law-making and it considers that cases can be adequately dealt with in the existing framework, that is, with defamation or the infringement of privacy.[74]

Furthermore, the MIC expects the self-regulation of the search engine service operators. The MIC put particular emphasis on the need to guarantee the transparency of the service by the search engine operators themselves, for example by clearly showing the criteria and the actual situation regarding information deletion. It can, therefore, be said that the actual situation of Japan is lead by the operators of the search engine service, not by any official authority.

To end this chapter, an interesting point should be noted.[75] So far, the right to be forgotten is claimed in the framework of civil responsibility, such as defamation or infringement of privacy. However, if it will become discussed in the context of the Act on the Protection of Personal Information, the problem will be of the nature of public law. The MIC—the ministry in charge—does not, at least so far, treat this question as one of public control. If this direction is changed, however, the tendency should be closer to the European approach, which protects personal information via regulation.

The root of the discussion is the question of the range of control of the individual.[76] To consider about this point, not only discussion in the civil law field but also that in the public law domain, such as public interest of the right to know, should be exhaustively covered. In any event, the discussion on the right to be forgotten in Japan remains immature and future developments need to be monitored carefully.

---

[72]Available in the Japanese language at http://www.soumu.go.jp/main_content/000369245.pdf. Accessed 27 December 2016.

[73]The Working Group Report (2015), p. 32.

[74]The Working Group Report (2015), p. 33.

[75]Sogabe (2016), p. 19.

[76]See Murata (2016), p. 531.

Acknowledgements This chapter is supported by the Research Grant-in-Aid of the KDDI Foundation.

References

Ambrose ML (2013) It's about time: privacy, information life cycles, and the right to be forgotten. Stanf Technol Law Rev 16:369–421

Ambrose ML, Ausloos J (2013) The right to be forgotten across the pond. J Inf Policy 3:1–23

Angelo M (2009) You are what google says you are. Wired, 11 Feb 2009. https://www.wired.com/2009/02/you-are-what-go/. Accessed 29 Sep 2016

Ausloos J (2012) The "right to be forgotten": Worth remembering? Comput Law Secur Rev 28:143–152

Beignier B (1992) Le Droit de la Personnalité. PUF Collection «Que sais-je?», Paris

Bennett SC (2012) The "right to be forgotten": reconciling EU and US perspectives. Berkeley J Int Law 30(1):161–195

Carter EL (2013) Argentina's right to be forgotten. Emory Int Law Rev 27:23–39

Cavoukian A, Wolf C (2014) Sorry, but there's no online "right to be forgotten." National Post, 25 June 2014. http://news.nationalpost.com/full-comment/ann-cavoukian-and-christopher-wolf-sorry-but-theres-no-online-right-to-be-forgotten. Accessed 23 Sep 2016

Duhiggfeb C (2012) How companies learn your secrets. The New York times magazine, 16 Feb 2012. http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?_r=0. Accessed 23 Sep 2016

Fazlioglu M (2013) Forget me not: the clash of the right to be forgotten and freedom of expression on the internet. Int Data Priv Law 3(3):149–157

Fiveash K (2011) Facebook tells privacy advocates not to "shoot the messenger." The register, 23 March 2011. http://www.theregister.co.uk/2011/03/23/facebook_shoot_messenger/. Accessed 21 Sep 2016

Freischer P (2011) Privacy…? Foggy thinking about the right to oblivion, 9 March 2011. http://peterfleischer.blogspot.jp/2011/03/foggy-thinking-about-right-to-oblivion.html. Accessed 21 Sep 2016

Fried C (1968) Privacy. Yale Law J 77(3):475–493

Guiton A (2015) « Droit à l'oubli »: Google dans le viseur de la Cnil. Libération, 12 juin 2015. http://www.liberation.fr/ecrans/2015/06/12/droit-a-l-oubli-google-dans-le-viseur-de-la-cnil_1328367. Accessed 28 Sep 2016

Gupta S (2013) The right to be forgotten. snIP/ITs: insights on Canadian technology and intellectual property law, 12 Dec 2013. http://www.canadiantechlawblog.com/2013/12/12/the-right-to-be-forgotten/. Accessed 21 Sep 2016

Hardy B (2014) Application dans l'espace de la directive 95/46/CE: la géographie du droit à l'oubli. Revue trimestrielle de droit européen 2014:879–897

Heisenberg D (2005) Negotiating privacy. Lynne Rienner Publishers, London

Hurst A (2015) Data privacy and intermediary liability: striking a balance between privacy, reputation innovation and freedom of expression. Entertain Law Rev 26(6):187–195

Jones J (2014) Control-alter-delete: the "right to be forgotten". Eur Intellect Prop Rev 36(9):595–601

Kanda T (2015) Net kensaku ga kowai: wasurerareru kenri no genjo to katsuyo [Scared of internet searches: the actual situation and application of the right to be forgotten]. Poplar Publishing, Tokyo

Kanda T (2016) Saitama Chisai Heisei 27 nen 12 gatsu 22 nichi kettei ni okeru "Wasurerareru kenri" no kosatsu [Analysis on the "Right to be forgotten" in the decision of the Saitama District Court of 22nd December, 2015]. Law Technol 72:41–46

Kranenborg H (2015) Google and the right to be forgotten. Eur Data Prot Law Rev 1(1):70–79

Lee J (2015) SB 508: does California's online eraser button protect the privacy of minors? UCD Law Rev 48:1173–1205
Marino L (2014) Un « droit à l'oubli » numérique consacré par la CJUE. La Semaine Juridique éd, Générale 26:1300–1303
Martinez CO (2015) The CJEU judgment in Google Spain: notes on its causes and perspectives on its consequences. In: Hess B, Mariottini CM (eds) Protecting privacy in private international and procedural law and by data protection. Routledge, Abingdon
Matsui S (2013) Hyogen no jiyu to meiyo kison [Freedom of expression and defamation]. Yuhikaku, Tokyo
Miller AR (1971) The assault on privacy. University of Michigan Press, Michigan
Miller LF (2009) Privacy in the public library. N J Lawyer Mag 260-OCT 19–23
Miyashita H (2016) Wasurerareru kenri to kensaku engine no hoteki sekinin [The right to be forgotten and legal responsibility of search engines]. Comp Law Rev 50(1):35–75
Mori R (2015) Kensaku to privacy shingai, meiyo kison ni kansuru kinji no hanrei [Recent cases on the searching and the infringement of privacy/defamation]. Horitsu no Hiroba 68(3):51–57
Morrison K (2015) Survey: many users never read social networking terms of service agreements. Social times, May 27, 2015. http://www.adweek.com/socialtimes/survey-many-users-never-read-social-networking-terms-of-service-agreements/620843. Accessed 4 Oct 2016
Murata K (2016) "Wasurerareru kenri" no ichiduke ni kansuru ichikosatsu [Analysis on the position of the "Right to be forgotten"]. Okayama Law J 65(3–4):493–531
Ogura K (2013) Internet jo no meiyo kison: saikin no futatsu no jiken ni tsuite [Defamation on the internet: an analysis of 2 recent cases]. Hogaku Semin 707:20–24
Picod F (2014) Renforcement de la responsabilité de Google et droit au retrait de données personnelles. La Semaine Juridique éd. Générale 1068:21–22
Promchertchoo P (2011) Facebook questions EU "right to be forgotten." TechWeek Europe, 23 March 2011. http://www.techweekeurope.co.uk/news/facebook-questions-eu-right-to-be-forgotten-24509. Accessed 21 Sep 2016
Prosser WL (1960) Privacy. Calif Law Rev 48(33):383–423
Purcell K, Brenner J, Rainie L (2012) Search engine use 2012, Pew Research Center's internet and American life project report, 9 March 2012. http://www.pewinternet.org/2012/03/09/search-engine-use-2012/. Accessed 26 Sep 2016
Richards NM (2005) Reconciling data privacy and the first amendment. UCLA Law Rev 52:1149–1222
Robertson E (2011) A fundamental right to read: reader privacy protections in the U.S. Constitution. Univ Colo Law Rev 82:307–330
Rosen J (2010) The web means the end of forgetting. N Y Times, 21 July 2010. http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html?pagewanted=all. Accessed 30 Jun 2017
Rosen J (2012a) The right to be forgotten. Stanf Law Rev Online 64:88–92
Rosen J (2012b) The deciders: the future of privacy and free speech in the age of Facebook and Google. Fordham Law Rev 80(4):1525–1538
Rubinstein IS (2011) Regulating privacy by design. Berkeley Technol Law J 26:1409–1456
Ryan T (2011) The right to be forgotten: questioning the nature of online privacy, 2 May 2011. http://www.psfk.com/2011/05/the-right-to-be-forgotten-questioning-the-nature-of-online-privacy.html. Accessed 21 Sep 2016
Saunders JL (2011) Across jurisdictions and web domains, questions of privacy and online anonymity persist, 15 April 2011. https://iapp.org/news/a/2011-04-15-across-jurisdictions-and-web-domains-questions-of-privacy-and/. Accessed 10 Jan 2017
Sogabe M (2016) Nippon ni okeru "Wasurerareru kenri" ni kansuru saibanrei oyobi giron no jokyo [The situation of cases and discussion on the "Right to be forgotten" in Japan]. Kangwon Law Rev 49:1–23
Solove DJ (2006) A taxonomy of privacy. Univ Pa Law Rev 154(3):477–560
Solove DJ (2012) Privacy self-management and the consent dilemma. Harv Law Rev 126:1880–1903

Valles CM (2001) Setting the course on data privacy as U.S. firms hesitate, EU gets set to enforce its rules an alternative voice. Int Her Trib 13, 28 May 2001 (SPECIAL REPORT)
Van Alsenoy B, Koekkoek M (2015) Internet and jurisdiction after *Google Spain*: the extraterritorial reach of the 'right to be delisted'. Int Data Priv Law 5(2):105–120
Volokh E (2000) Freedom of speech and information privacy: the troubling implications of a right to stop people from speaking about you. Stanf Law Rev 52:1049–1124
Walsh J (2011) When it comes to Facebook, EU defends the "Right to disappear." The Christian Science Monitor, 6 April 2011. http://www.csmonitor.com/World/Europe/2011/0406/When-it-comes-to-Facebook-EU-defends-the-right-to-disappear. Accessed 21 Sep 2016
Warren SD, Brandeis LD (1890) The right to privacy. Harv Law Rev 4(5):193–220
Westin AF (1967) Privacy and freedom. Ig Publishing, New York
Whitman JQ (2004) The two western cultures of privacy: dignity versus liberty. Yale Law J 113:1151–1221

Part II
Innovation Intermediaries

Intermediaries and Mutual Trust: The Role of Social Capital in Facilitating Innovation and Creativity

Shinto Teramoto and Paulius Jurčys

Abstract What are the key factors that facilitate innovation and creativity? This chapter begins by challenging the traditional emphasis on IP rights as an incentive to creators to innovate. While it is true, that IP rights provide for a much-needed tool to protect creative ideas, we argue that a much more important policy objective is to facilitate the dissemination of ideas in the society. Moreover, we submit that in the age of networked societies, dissemination of ideas could be facilitated by creating a trust-based ecosystem with different incentives for various kinds of intermediaries to emerge and compete with each other and making sure that users are actually able to choose through which intermediary information should be accessed or disseminated. We begin this chapter by offering a brief exposition of the notions of social capital and mutual trust. Mutual trust is a complex phenomenon involving multiple stages of cognitive decisions between a trustor and a trustee. The degree of trust evolves over time and is based on the experience between the communicating parties. Accumulation of trust between members of a society (a kind of social capital) significantly contributes to sharing of ideas and enhances cooperation. In more complex societies, trusting one's neighbor (intermediary) is one of the major factors that minimizes risk and facilitates communication through neighbors (intermediaries). In designing a trust-based innovation ecosystem, it is first of all important to identify the relevant stakeholders and their main interests. Such stakeholders and their interests may vary depending on their geographical location or the market in which they are operating. We argue that innovation thrives in more flexible regulatory environments, which pose less restrictions and are able to swiftly adjust to the changing needs of technological evolution. Moreover, we suggest that regulators should aim to create ecosystems where more intermediaries could emerge and compete with each other. Having multiple intermediaries enables users to choose whom they believe to be able to provide higher quality products and

S. Teramoto
Graduate School of Law, Kyushu University, Fukuoka, Japan

P. Jurčys (✉)
Popvue Inc., San Francisco, USA
e-mail: pjurcys@gmail.com

M. Corrales et al. (eds.), *New Technology, Big Data and the Law*,
Perspectives in Law, Business and Innovation, DOI 10.1007/978-981-10-5038-1_6

services. Higher level of trust between various stakeholders of ecosystem contributes to sharing, collaboration, dissemination of information and innovation.

Keywords Intermediaries · Mutual trust · Social capital · Innovation · Creativity

Contents

1 Introduction

On 12 June 2014, Tesla's CEO Elon Musk announced that his corporation "will not initiate patent lawsuits against anyone who, in good faith, wants to use [Tesla's] technology."[1] Even though he described IP as a "landmine" which does not necessarily contribute to the advent of technology, Musk noted that the real competition comes not from competition among electric car manufacturers, but competition among manufacturers of diesel and electric cars. Besides, Musk pointed that:

> Technology leadership is not defined by patents, which history has repeatedly shown to be small protection indeed against a determined competitor, but rather by the ability of a company to attract and motivate the world's most talented engineers. We believe that

[1]See Musk, *All Our Patent Are Belong to You*, available at: http://goo.gl/Eb3OQe. Accessed 10 January 2017. Tesla is not the only company which has chosen to disclose its technology. For instance, one of the leaders in the air conditioning market—Japanese corporation Daikin—announced that it will engage in open licensing of its HFC-32 technology for making next generation energy-efficient air conditioners, see *Efficient Air Conditioning for the Next Decade*, available at: goo.le/6QuazrO. Accessed 10 January 2017.

> applying the open source philosophy to our patents will strengthen rather than diminish Tesla's position in this regard.[2]

This statement highlights some of the most notable developments with regard to the role of IP rights in stifling innovation. Recently, however, such a common opinion has been increasingly criticized arguing that IP rights often create more hurdles to innovation than add stimulus. This chapter begins by providing a critical account of the role of IP rights and rules governing unfair competition as legal tools that are supposed to stifle innovation. Acknowledging the significance of IP rights and competition law, this chapter points out that the prevailing theories of IP rights do not provide a clear-cut explanation about the origins of creativity, innovation and the reasons why people engage in creative activities.

This chapter shows that besides IP rights, multiple other factors and policy measures contribute to creativity and innovation. In particular, it is suggested that the success of collaboration in creative endeavors very much depends on the dynamics of interpersonal relations and mutual trust among creators as well as other participants in the innovation ecosystem. Individuals who trust each other are more likely to come up with creative ideas and materialize them. In the academic literature, mutual trust is studied as a form of social capital.[3] Social capital offers a dynamic perspective on inter-personal relations and could be employed as a tool to better understand the upshots of creativity and economic growth.[4] Yet, there has been little attention devoted to social capital in IP-related academic scholarship.[5]

This chapter aims to contribute to the debate and discusses the role of intermediaries who play a key role in disseminating information. A closer look at changes in the publishing businesses illustrates that non-legal factors such as mutual trust help reduce transaction costs and open new opportunities to share information. This paper offers some considerations about the possible improvements of the legal framework to help in the accumulation of social capital and creativity. The main claim is that the legal system should be more amenable to creators' choices in building new frameworks of collaboration and dissemination of information. Focusing on employee inventions and commercialization of innovative ideas, we introduce seven different categories of rules in order to show the multiple dimensions where trust-based relations play a particularly important role. It is submitted that an innovation-friendly legal framework should pay greater respect to creators' choices.

---

[2]See Musk.

[3]See, e.g., Lin (2001), Ostrom and Ahn (2003).

[4]Leading scholars have identified various constitutive elements of collaboration online. For example, Yochai Benkler distinguished the physical layer, logical layer and the content; see Benkler (2006). Prof. L. Lessig is known for analyzing four modalities of constraints for human behavior in cyberspace (namely, law, markets, social norms and architecture), see Lessig (1999). The importance of mutual trust is also fragmentarily noted Jonathan Zittrain, see Zittrain (2008).

[5]See Teramoto and Jurčys (2014), Teramoto et al. (2014).

2 Changing Landscape of Innovation Ecosystems

The statement of Elon Musk perfectly defines the current state of the debate about the role of IP rights. Recently, the view holding that IPRs incentivize innovation has lost much of its attractiveness. This is partly due to the changing architecture of innovation, the emergence of the Internet, Big Data and proliferation of open innovation. Tesla's CEO is also right when he talks about IP rights as landmines to innovation for IP rights may indeed be abused by non-practicing entities.[6] The shift whereby firms disclose their core technology is possible when so-called "first movers" are able to set forth industry standards and reap benefits once those standards gain wide acceptance in the market. Yet, first mover advantage is contingent upon the availability of appropriable technology, market circumstances, marketing strategies and deep pockets of the company.[7] Even if firms choose to disclose their technology, they may still employ protection afforded by IP rights and unfair competition rules. The interface between these two sets of norms and their ramifications to creativity are discussed hereinafter.

2.1 IP Rights, "Free" Competition and Innovation

IP and competition law play a significant role in facilitating innovation. IP rights are crucial at the seed-stage of innovation when the creative ideas have to be protected. Besides, various contractual mechanisms help to secure that the information that is vital to the firm does not leak. Non-disclosure agreements are signed at the initial stages of collaboration—be it start up firms of large entities entering into licensing negotiations. Possession of IP rights is but one of the factors taken into account by venture capitalists who decide whether to invest into the next round of Research and Development (R&D). IP rights also offer a powerful weapon against competitors who free ride and exploit the IP-protected technology. Nevertheless, Venture Capitalists (VCs) often tend to give greater weight to such factors as the presence of a viable business plan, a highly skilled and trustworthy management, good reputation and strong tries to the industry leaders.[8]

There is a considerable overlap between the goals of IP and competition law: both aim to promote innovation and growth. IP rights enable inventors to enter the market and recoup their investments by selling innovative products. Once the firm manages to achieve considerable market power, unfair competition/antitrust law becomes of paramount importance. Competition law provides safeguards in cases where the market is already ripe but there is a need to shield-off unfair competitors.

---

[6]Bessen and Meurer (2008), see also Balganesh (2013).

[7]Suarez and Lanzolla (2005), Lieberman (2014).

[8]See, e.g., Burstein (2012).

The promotion of social welfare and innovation rests upon the effectiveness of IP and competition laws. IP rights provide a strong incentive to innovate especially in high-tech industries. Stronger IP protection stifles innovation and increases profit from initial innovation, but may hinder follow-on innovation. Conferring strong IPRs for initial innovation makes it less likely that there will be subsequent imitation by the producers of inferior technologies.[9] Once the IP-protected product is developed and distributed, the IP-right holder can control the dissemination of products by refusing to deal with price-setting.

Firms may employ various tools trying to restrict the conduct of competing IPR-holders (e.g., refusal to deal, setting unfairly high prices or imposing certain restrictions upon licensees).[10] Economists have analyzed the refusal to deal by drawing a line between upstream and downstream markets. The upstream monopolist may refuse to deal with downstream rivals when there is likelihood that there will be a follow-up innovation in the upstream competition. In such cases, the upstream monopolist aims to get short-term benefits but this negatively affects consumer and social welfare especially if the likeliness of follow-up innovation is low.[11]

The debate over the interface between competition and IP law turns around the question whether a monopolist should be compelled to share its IP with its rivals; and, if so, under what conditions.[12] Vertically integrated firms may refuse to deal downstream to downstream rivals in order to maintain vertical control in the presence of potential upstream competition.[13] Strict limitations on the pricing may negatively affect incentives to innovation and thus reduce consumer and social welfare.[14] In cases where there is a strong antitrust policy and strict anticompetitive conduct regulation means that there is less desire to have strong IP protection[15] (Fig. 1).

The graph above highlights that much innovation occurs between the two extremes of "fierce" and "soft" competition. In the zone of "free" competition, the companies are building their second or third generation products and try to seize more market power. Rent-seeking is one of the key reasons why at the stage of "free" competition the rival companies are not willing to compete each other (therefore, we can define this stage of competition as "no competition"). This idea

[9]Burstein (2012), p. 538.

[10]Chen (2014).

[11]Chen (2014), p. 536.

[12]Vickers (2010). The answer to this question depends on numerous practical circumstances of the case. In the US, it is commonly agreed that the right-holder can refuse to deal with competitors and that such a refusal does not violate antirust laws. See, e.g., *CSU, L.L.C. v. Xerox Corp.*, 203 F.3d 1322 (Fed. Cir. 2000); *Verizon Communications Inc. v. Law Offices of Curtis V. Trinko LLP*, 540 US 398 (2004). However, EU regulators have been more restrictive with regard to the scope of monopoly powers of dominant undertakings, see EU *Microsoft* case.

[13]Chen (2014), p. 537.

[14]Chen (2014), p. 545.

[15]Chen (2014), p. 549.

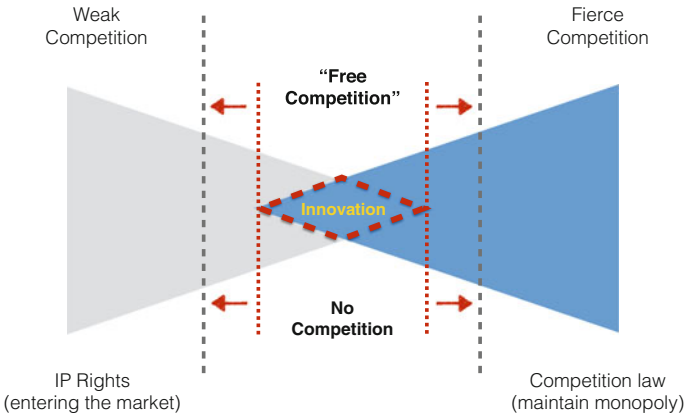

Fig. 1 The role of IPRs and competition law in fostering innovation

of the degree of "free competition" offers much food for thought whether, and under what conditions the boundaries of free/no competition should be expanded or curtailed and what degree of regulation is desirable. Yet, as it will be shown below, the current literature does not explain the roots and upshots of creativity and innovation.

2.2 *Missing Bits and Pieces of Philosophical Justifications of IP Rights*

The prevailing view is that both IP law and competition law create economic incentives to innovate; besides, it is widely assumed that IPRs system aims to balance the interests between the monopoly right-holders and the market.[16] Recently conducted case-studies have shown that this incentive-based approach offers little explanation about the inspired beginnings of creativity and the functioning of complex innovation ecosystems.[17] Some scholars also found that IP rights play a rather small role in the digital environment or modern arts.[18]

There are three main theories justifying the existence of IPRs system: fairness/labor theory, personality theory and welfare theory.[19] The proponents of the fairness theory submit that each person has a claim to the fruits of her

[16]Landes and Posner (2003).

[17]See, e.g., Lobel (2013), Silbey (2014).

[18]Gervais (2012).

[19]Hughes (1988), Merges (2011).

(intellectual) labor whereas the state has a duty to enforce those rights.[20] Accordingly, each person deserves a share of the fruits of the work proportionate to the magnitude of her contribution to the venture. Following Locke's view, the creators of innovative content should be entitled to bear the ownership to such works and get reasonable compensation.[21]

The so-called "personality" theory emphasizes the deep emotional connection between the creator and the creative work. The work is deemed as a manifestation of the creator's personality; the creator expresses herself through created pieces of art. Therefore, creators should be entitled to "own" their creative products. One of the distinctive features of personality theory is that it emphasizes the importance of moral rights.[22]

The foundations of the most pervasive welfare theory can be found in the works of Jeremy Bentham[23] and John Stuart Mill.[24] Both of them were concerned about the distribution of resources in the way that would confer greatest happiness to the greatest number of people. The proponents of this utilitarian approach posit that the law should "nudge" people in a socially beneficial direction. This theory is prospective and oriented to the welfare of the society as a whole. In order to solve the problem of under-production and under-innovation, the government is urged to take active steps to create incentives (e.g., IPRs) that would facilitate the efficient allocation of resources in the community.

These three philosophical approaches help us better understand the rationales underlying the IP regime; yet they bear little connection to creativity itself. In recent years, there has been an increasing interest in studying the motives and circumstances that trigger human creativity. Scientists across various disciplines have been wondering what makes people create at the first place? Is creativity an everyday strand for creators and innovators? Are creative ideas always the outcome of conscious thinking? How could the surrounding environment facilitate the breeding of creative ideas?

In her recent study, Jessica Silbey offered a compelling account about the roots and offshoots of creativity.[25] Her empirical and qualitative claim is that there are three motivations to create: (1) plays and lucky accidents; (2) problem-solving; and (3) pleasure seeking and challenging oneself.[26] Traditional IP regimes attach very little, if any, importance to such "eureka moments"; although being "first-in-time" may play a crucial role in getting IP protection. Artists often merely want to express themselves, and seem to be quite tolerant of copy-cats. If possible, artists want to

[20]Locke (2010), Chap. V; see also Damstedt (2003), McGowan (2004), Zemer (2006), Mossoff (2012).

[21]See Merges (2007).

[22]Rigamonti (2006).

[23]See Bentham (1996).

[24]Mill (1998).

[25]Silbey (2014), Chap. 1.

[26]Silbey (2014), Chap. 1.

publish their works and see them disseminated. Rather than seeking to own their works, they first and foremost seem care more about attribution.[27] The satisfaction which creators feel in the mind-bending process or knowing that there is a problem they managed resolving inspires creativity more than anything else.

3 The Notion of Mutual Trust

As the previous section has illustrated, currently prevailing justifications only partially explain the origins of innovation. This chapter aims to suggest that besides IPRs and other economic measures, innovation and creativity is more likely to occur in societies with greater accumulation of social capital and mutual trust. In fact, social capital has been one of the missing pillars in the IP literature on innovation creativity.[28] Mutual trust lies at the heart of human relationship (among family members, friends as well as in corporate environment) and therefore deserves more attention. The following sections briefly outline the main features of social capital and aims to explain the added value of this concept in understanding the processes of collaboration and innovation.

3.1 Shifting Focus to Social Capital and Mutual Trust

The foundations of studies on social capital lie in the rich literature of economics,[29] sociology,[30] psychology, political sciences,[31] etc. In the middle of the twentieth century when economists embarked on studying the decision making within corporate settings.[32] Firms were viewed as vertically organized structures with top-down decision-making and hierarchically enforced rules. The key question in production process is whether a firm should produce by itself or outsource others. Coase made a visionary observation that when costs of bargaining are relatively high, firms tend to choose to produce themselves. However, if transaction costs are low, firms are more willing to collaborate with each other.

[27] Silbey (2014), p. 27.

[28] Some fragmentary references to the importance of trust among the players in the innovation ecosystem could be found in the innovation-related literature, see, e.g., Hwang and Horowitt (2012).

[29] Williamson (1993), Dasgupta (2005), Dasgupta and Serageldin (2000).

[30] See, e.g., Luhmann (2000), Sztompka (1999), Solomon and Flores (2003).

[31] Coleman (1988) and, more fundamentally, Coleman (1990).

[32] See, e.g., Coase (1937, 1960).

The debate about firm structure and intra-firm interaction was advanced by Oliver Williamson.[33] He showed that intra-firm relationships are often based on incomplete contracts and that firms have only limited abilities to act rationally. In long-term relationships, firms often rely on informal routines and mutual trust among the firms was identified as having paramount importance.[34] These findings were further substantiated by political scientists who studied the governance of common pool resources (such as forests or land) and also found that mutual trust plays a central role in large and complex societies.[35]

3.2 *Multi-Layered Notion of Mutual Trust*

One of the core categories of social capital is mutual trust.[36] The category of trust is one of the powerful tools that helps better understand interactions between the participants in the innovation ecosystem (creators, employee-inventors and their employers, as VCs and government). Trust also provides a new angle to analyze how their interaction evolves over time and how such phenomena as power, norms or emotions influence creativity.[37] In the following sections we will show that mutual trust is a complex concept entailing multiple dimensions: cognitive, affective and social.

Recently conducted empirical studies generated a great deal of content-specific definitions of trust. Initially, it might be helpful to highlight the distinction between trust as an *attitude*, and trust as an *act*. Trust as an "attitude" refers to the emotional and psychological feeling of the trustor, whereas trust as an "act" defines the actual decision to rely upon someone. Hence, the act of reliance is contingent on the trustor's psychological attitude towards the trustee.[38]

There is no single notion of trust but some more widely accepted definitions should be noted. For instance, Gambetta focuses on the belief of the trustor and the probability that the trustee will help achieve certain results, which increase both of their welfare.[39] Others emphasize that trust is a decision based on certain valuation; by deciding to trust another person the trustor is aware about possible risks that may emanate due to the reliance on such person.[40] This notion raises a question how a decision to trust is influenced by surrounding circumstances and trustor's

[33]Williamson (1998, 2010).

[34]See Williamson (1983, 1993, 2010).

[35]Ostrom (2005), p. 69, Ostrom (2010).

[36]For various definitions of social capital, see, e.g., Putnam (1994), Bowles and Gintis (2002), Nahapiet and Ghoshal (1998).

[37]Castelfranchi and Falcone (2010), p. 2.

[38]Castelfranchi and Falcone (2010), p. 18.

[39]Gambetta (1988), Castelfranchi and Falcone (2010), p. 22.

[40]Mayer et al. (1995).

behavioral weaknesses or biases (e.g., lack of attention or wrong perception of risk).[41] Some take a rather narrow approach and define trust as risk-taking "on the expectation that the others will reciprocate."[42] Hardin persuasively defines trust by focusing on goal-adaptation. This means that the trustee (agent) takes into consideration the interests (needs, desires, projects, etc.) of the trustor and acts accordingly.[43]

From the definitions above, we can surmise that trust entails three main constituents: (1) a mental attitude towards the agent; (2) the trustor's decision to rely on the trustee; and (3) intentional act of trusting and the consequent interaction between the trustor and trustee.[44] The root of trust lies in trustor's beliefs and opinion (which may be false, although rational and justified) about the trustworthiness of the trustee.[45] In deciding whether the agent is trustworthy, the trustee considers trustee's competence and willingness to act in the interest of the trustor as well as whether trustee's actions are predictable. Trustor's final act of delegation depends on the positive appraisal of the trustee as having the necessary qualities to achieve trustor's contemplated goal.[46]

3.3 Trust, Expectations and Risk

Using social capital and mutual trust provides an extremely useful set of tools to explain the dynamism of social interactions. In considering the possibilities of the realization of the goal, the trustor may have four expectations: positive or negative (i.e., whether the goal will be realized and fear that it may be not achieved), neutral and ambivalent. Such expectations may have different intensity in terms of how much joy, relief, frustration or disappointment they may cause. While goals can have a monetary certain value (agent's failure could be assessed monetarily); the effects of disappointment if that goal is not achieved often are subjective and intangible.[47]

In many situations, the lack of trust exists because of information asymmetries. In a highly risky and uncertain world, distrust could be seen as the default; yet trust-based relations form bridges between familiar and unfamiliar and help reduce

[41]Castelfranchi and Falcone (2010), p. 20.

[42]Levi (2003), p. 382.

[43]Hardin (2002). Hardin's embedded interest approach has provided a basis for further studies in the area of cooperation theory and general sociology and highlights the fact that surrounding circumstances or behavioral biases affect trustee's behavior. See, e.g., Tuomela (1993), Castelfranchi and Falcone (2010), p. 27.

[44]Castelfranchi and Falcone (2010), p. 35.

[45]Castelfranchi and Falcone (2010), p. 39.

[46]Castelfranchi and Falcone (2010), pp. 43–47.

[47]Castelfranchi and Falcone (2010), p. 119.

risk.[48] Trust is also closely related to confidence. The breach of trust or confidence would always end in disappointment. The distinction between the two could be best made having regard to dangers and risks.[49] Dangers exist naturally and are independent from the choices of people; whereas risk arises in situations when individuals have to make choices. One classical example is a parents' risk in leaving their child with a babysitter whom they trust without knowing whether the babysitter may be a serial killer.

3.4 Autonomy, Delegation, and the Dynamic Aspect of Trust

While hierarchical relations are based on power, control and fear, mutual trust is a cornerstone element in building peer-to-peer relations.[50] Greater trust among the employees and management incentivizes employees to perform better, motivates them to be creative and increases efficiency. However, some additional explanation is needed to define the interplay between mutual trust and autonomy. Assume a situation where the trustor has to make an action decision. There are three possible ways to solve the problem: (1) the trustor can perform an action by himself; (2) delegate tasks to a trustee; or (3) to do nothing (abstain from taking any action). In the case where tasks are delegated to an agent, the degree of trust also defines how much autonomy is bestowed upon that agent. In other words, less trust in the agent could mean that certain control mechanisms over the execution of the delegated task could be imposed (e.g., give ex ante instructions or require periodical reports).

To sum up, trust highlights the dynamic nature of human interaction. Trust is an epistemic notion; it is built and adjusted over time depending on the pre-existing relationship between trustor and trustee. Hence, the trust decision is a voluntary choice. In the absence of trust, there is only fierce competition and hidden sabotage; there is no possibility of cooperation and there are very few winners and many losers. The following sections look into the more practical issue of how trust in intermediaries relates to collaboration and dissemination of information.

[48]Luhmann (2000), p. 95. This familiarity-trust dichotomy helps demonstrating that trust is only possible in the familiar world; therefore, familiarity is a necessary precondition for trust or distrust, see Luhmann (1979), pp. 19–21.

[49]Luhmann (2000), pp. 97–98.

[50]An exposition of how one of the leading IT corporations has managed to build a peer-to-peer collaborative work environment see, e.g., Schmidt and Rosenberg (2015), Bock (2015).

4 Innovation Intermediaries and Mutual Trust

In the previous section, we introduced the notion of social capital and mutual trust. Social capital refers to the values that are embedded in networks and trust-based relations among network members. This section will illustrate the significance of social capital and trust in complex network settings with multiple actors. In particular, this section will focus on social interactions involving intermediaries who play an important role in large groups of actors. The first part of this section will illustrate how the Internet and Cloud computing transformed the modes of dissemination of information thanks to the emergence of the Internet intermediaries. The second part of this chapter will show that most of the creators who are keen to make sure that their works reach the audience prefer to move closer to intermediaries that are must trusted in the market. The power of social capital in the context of creativity and disseminating information will be illustrated by addressing recent changes in the music publishing business.

4.1 Network Structure and the Bridging Role of Intermediaries

The development and proliferation of digital communication technologies opened enormous opportunities for creating and disseminating information. This wealth embedded in networks has tremendous effects on the global economy as well as various features of social life. There are myriads of opportunities in the highly interconnected world; all you need to do is to turn the switch on and know whom to connect with. In the ideal world, it would be perfect if everyone knows everyone else, then the costs of communication and the risk of error would be reduced to minimum. In reality, however, most digital communications occur via intermediaries who provide platforms or render services that assist communication. Such a communication system is probably the second-best mode of communication because the distance between two actors connected by an intermediary is two steps (a so-called "hub-and-spokes" network).[51]

The emergence of the Internet, Cloud computing and "Big Data" has fundamentally altered the ways for the information exchange. In the age of digital communications, online intermediaries offer shortcuts (i.e., lower costs and better quality) between remote actors in communication networks. For instance, online intermediaries have disrupted traditional publishing businesses. Traditionally publishers arrange printing of the manuscript as well as the dissemination of the work through various distributors such as bookshops. The public can also access those publications by other channels (e.g., libraries, or second hand book-shops). Thanks

[51]For a more detailed account, see Teramoto and Jurčys (2014), pp. 99 et seq.

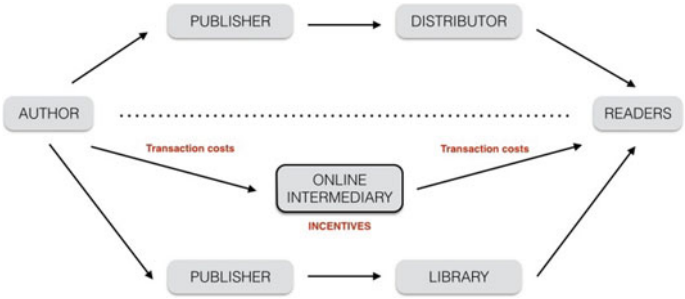

Fig. 2 Disruptive effects of emerging online intermediaries

to the emergence of online intermediaries, creators now have more alternative ways to disseminate their works to the audience (e.g., uploading directly to online sites and sharing for free) while traditional business operators had to adapt their business models in order to remain in the market (Fig. 2).

Intermediaries who manage to fill in the gap in a network and manage to establish bridges between different members of the network are very likely to become brokers and earn huge payoffs.[52] In the social networks literature, such intermediaries are defined as "structural holes" because the absence of those intermediary network members would only know their adjacent members.[53] Intermediaries who become "structural holes" enable the network members to access new pools of information (e.g., download music, or get information about employment opportunities) and do it at a significantly lower cost. The existence of structural hole also helps harvest social capital in the community.[54] In social reality, networks of collaborations that are bridged by structural holes are more apt to learning, adaptation and creativity. The same is true in inter-organizational settings. Communities with heterogeneous mix of ties are more likely to develop new ideas. Moreover, empirical studies have demonstrated that actors located in a closed network are more likely to come up with better ideas.[55]

4.2 Intermediaries, Growth and the Value of Social Capital

From a regulatory point of view, the obvious objective of any regulator is to create an environment where intermediaries are facilitated to test new waters and fill existing communication gaps by developing new highways of interaction. From the

[52]Kleiberg et al. (2009).
[53]Burt (2004).
[54]Granovetter (1973).
[55]Burt (2004), p. 379.

social welfare point of view, the existence of multiple alternative ways to disseminate creative content is very much desirable. Thus, governments could and should be thinking about the need to create an environment where as many as possible new intermediaries are established and compete with each other. In the above-given publishing example, the society benefits most if there are multiple ways to access information (e.g., purchasing books in bookstores and online, second-hand book markets, borrowing at the libraries, etc.).

Since the emergence of the Internet, there has been also a shift in the notion of appropriation of revenues. Conventionally, creators sought to appropriate internal knowledge by obtaining IPRs and commercializing them. In an open innovation world, creators tend shift their focus from appropriation of IPRs towards appropriation of revenues. Hence, IPRs rights become a kind of a tradable asset.[56] Growth has become the buzzword, which explains the existence of corporate entities.[57] The success of the firm is no longer measured by how many patents or end products the corporation has developed, but by how much value the business model of a company can generate. Growth vectors infuse optimism for closer cooperation within the firm and also attract much-sought resources from VC.[58]

Probably one of the most telling illustrations of the importance of intermediaries in the dissemination of information, pursuit or revenues of importance of trust could be found in distribution of audio-visual recordings. Traditional music distribution models have been disrupted by sudden rise of such online intermediaries as YouTube, iTunes, Spotify and Pandora. They have suddenly become major market players and practically rendered hard copies or recordings futile. Most of the creators usually moved to disseminate their records via abovementioned online intermediaries. In terms of structural holes theory, the abovementioned intermediaries have become major players in the market. Although their business models differ, over time they have acquired great trust both from the side of creators and various contingents of audiences.

The A graph below depicts a situation where a major publisher A is positioned as a structural hole and has close connections with authors, distributors B, C, and D as wide audiences of readers. This graph could be adjusted to fit the digital publishing environment by replacing A, B, C, and D by a single intermediary such as Spotify. In the reality, the situation would be much more complex than the graph below because multiple online intermediaries exist side-by-side together at the same (Fig. 3).

[56]Chesbrough et al. (2006).

[57]McCahery and Vermeulen (2014).

[58]Such focus on growth and revenues could be noted in the film industry: in order to reap the greatest amount of revenues, studios often choose to release a movie in different windows at a different time-windows (firstly, in theatres, then pay TVs, pay per view, airlines, television networks, video stores, cable companies). See Fisher (2004), p. 213.

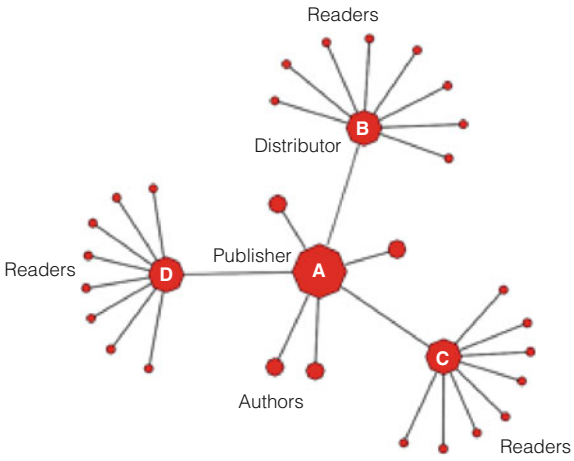

Fig. 3 A graph illustrating several kinds of structural holes

The dynamics of the relations between various actors in the music industry could be well illustrated by a recent decision of Adele not to allow streaming her third album "25" on Apple Music and Spotify.[59] Adele's decision was based not only upon economic estimates, but also her biggest strength—fame and wide appeal.[60] Adele's music is popular both among teenagers who use YouTube on a daily basis as well as older fans. The decision not to allow online streaming shattered the sales record for opening week sales, which was set in 2000 by the boy band N'Sync reaching 3.8 million copies.

Adele's case study serves well to illustrate the power of social capital. Rather than submitting itself to the rules which are set by market players (publishers, record labels and other intermediaries), Adele was able to resort to her accumulated social capital and world-wide appeal to put a halt to the online music industry, which is gradually leaning towards online content streaming. In particular, artists with a significant amount of accumulated social capital can pose serious competition to the intermediaries themselves. Although accumulating trust and reputation can take years, once creators accumulate such social capital they can utilize it not only for their own benefit, but also to influence the processes of standard setting in the industry. In fact, few weeks after the release of Adele's album, Spotify announced changes to its publishing rules to allow some artists to release only on pair tier.[61]

[59]See http://goo.gl/gZ3C68. But Adele was not the first one to do so: earlier in 2014, Taylor Swift also refused to allow streaming her new album "1989" on Apple Music, see http://goo.gl/3mYIRy. Accessed 10 January 2017.

[60]Lucas Shaw, *Why Adele isn't Streaming Her New Album Spotify or Apple*, see http://goo.gl/EHgjtg. Accessed 10 January 2017.

[61]See http://goo.gl/fo9lTC. Accessed 10 January 2017.

5 Designing a Trust-Based Innovation Ecosystem

Governments around the world are actively trying to boost creativity by opening special economic zones and offering incentives. For instance, in 2010 the local government of Fukuoka—a city located in the South West of Japan, decided to take active steps to turn the whole region into a South-East Asian innovation hub. Building the next generation Silicon Valley may be a daunting ambition, which depends on various exogenous factors (local climate, cultural and historical background of the area, economic and geo-political situation, available natural resources etc.). It is therefore recommended to adopt a functional approach and consider what elements are vital to the functioning of the innovation ecosystem. This chapter suggests that the legal system should be designed in a way that enables creators to engage in new forms of collaboration. More particularly, it is argued that innovation tends to thrive more in environments where the degree of social capital and mutual trust is higher. After discussing the role of major players in the innovation ecosystem, this section draws attention to seven categories of rules that should be designed in a way so that choices made within the creative communities could be legally incorporated in the architecture of innovation ecosystem.

5.1 Main Players in the Innovation Ecosystem

Each innovation ecosystem contains six main actors who perform different functions. Universities and academic institutions are probably the most important group players. Advanced research activities are usually conducted in universities, which are also the place where the brightest young minds gather. Universities put a lot of effort to maintain close contacts between the academic community and businesses by organizing various conferences and joint collaboration projects. Besides, universities also try to maintain a creative environment for research purposes and give much attention to the commercialization of university-generated innovation.

Humans by nature are curious and knowledge-seeking. Yet, it is important to acknowledge that in most cases financial considerations bring like-minded people together to form new start-ups or join large corporations. The possibility of earning money also depends on the ability to be the first in uncovering new markets. Yet, many skills and much investment are required in order to materialize an abstract idea. Creators who have little business experience often avail themselves to innovation intermediaries (such as consulting companies or lawyers) or incubators who help crystallize a business plan, establish a corporation or search for investors.

Creative ideas may pop-up suddenly, however, it my take time until those ideas turn into successful technology or piece of art. Innovation incubators offer facilities, necessary equipment and networking opportunities to bring the R&D project to the next stage. Greentown Labs facility in Cambridge, MA is a great illustration of such

an innovation incubator.[62] Greentown Labs hosts start-up companies that are developing next-generation green technologies (wind turbines, energy storage batteries, etc.). Start-up companies pay a small fee for which they have a desk, know-how and necessary R&D facilities. Many other innovation intermediaries maintain close ties with Greentown Labs and offer their services to those start-ups. There are also regular workshops, fairs and conferences in order to facilitate interdisciplinary collaboration.

VC firms provide funding to founders of start-ups. But, the function of VC firms is much more far-reaching: they help distill entrepreneurial endeavors, which have potential to turn into successful business models. After the initial/seed rounds of investment, VCs obtain control rights in the firm (e.g., right to appoint board members or monitor and direct the implementation of the business plan). Last but not least, innovation ecosystems depend on the leadership of the government. The government plays a key role in defining the legal frameworks and establishing favorable conditions for the transfer of technology, capital and resources.

However, even if all of these players gather together, this does not mean that innovation ecosystem will flourish. The main argument here is that social capital and mutual trust are crucial in building a next generation Silicon Valley. However, mutual trust and social capital require much time and effort, shared interest and repetitive interaction among the members of the innovation community. From a legal point of view, it must be analyzed how legal systems could be adjusted in order to facilitate the generation of trust and accumulation of social capital.

5.2 Choice Architecture, Social Capital and the Law

Previous chapters have shown multiple ways in which intermediaries and social capital contributes to the welfare of the society: the ease of communication not only reduces transaction costs but also opens opportunities to access diverse information. These ideas sound great and appealing. Yet, the question remains—how could law contribute to the proliferation of intermediaries and accumulation of social capital in society? Moreover, if ease of communication, dissemination of ideas and favoring disruptive innovation are at the forefront of the political agenda, how could these goals be achieved by legal or regulatory means?

This section shows that besides economic incentives, a far-fetching objective to spur innovation could be implemented by improving legal system and making it more receptive to individual's choices. This means that new opportunities are also posing challenges to existing regulatory framework. In order to substantiate our main claim, we rely on previous studies conducted by economists who have identified seven main categories of rules that affect the actor's behavior and decision-making.

[62]See http://greentownlabs.org. Accessed 10 January 2017.

Together with her colleagues, Nobel-winning institutional economist Elinor Ostrom conducted multiple empirical studies with regard to the governance of common pool resources (such as irrigation systems, beaches, forests, etc.) in different countries and communities. After many years of investigation, Ostrom developed a general scheme that explains factors that affect any form of governance of common pool resources.[63] Besides, Ostrom's model of governance highlights seven types of "exogenous" rules that affect any governance mechanism:

1. *Boundary rules* that specify how actors are to be chosen to enter or exit the positions they hold;
2. *Position rules* that specify a set of positions and how many actors could hold each of those positions;
3. *Choice rules* that specify which actions are assigned to an actor in a position;
4. *Information rules* that specify channels of communication among actors and what information must, may or must not be shared;
5. *Scope rules* that specify the outcomes of that could be affected;
6. *Aggregation rules* that specify how the decisions of actors at a node are to be mapped to intermediate or final outcomes (e.g., majority or unanimity rules); and,
7. *Payoff rules* that specify how benefits and costs are to be distributed to actors in positions[64] (Fig. 4).

Based on her empirical findings, Ostrom noted that in situations where individuals and societies are facing tough dilemmas, the role of mutual trust is expected to attain paramount importance. Mutual trust helps individuals devise more efficient interaction mechanisms and enhance transactional outcomes.[65] Increased level of mutual trust help people learn from each other and adopt norms that facilitate cooperation.

The taxonomy of seven categories of rules introduced above provides for a fertile ground in thinking about the architecture of innovation ecosystem. An individual's decision to act or to collaborate with other actors is based on calculations and expectations about the future benefits of a certain transaction as well as available information. Therefore, information and aggregation rules should be transparent and foreseeable so that actors in an innovation ecosystem could easily figure out the regulatory requirements. Besides, the aggregation rules should ascertain that agreements entered by those individuals are enforceable.

In creative economies, ideas are the most valuable asset. In addition, being the first in the market is of crucial importance. Therefore, rules setting the boundaries of

[63]Ostrom called that scheme "action-situation" and noted that in studying any kind of game, it is necessary to identify the following factors: characteristics of actors involved in the game; positions they hold (e.g., first mover or row-player); the set of actions that actors can take as specific nodes in a decision tree; the amount of information they possess; the outcomes that actors jointly affect; the set of functions that map actors and actions at decision nodes into intermediate and final outcomes; and the benefits and costs assigned to the linkage of actions chosen and outcomes obtained. See Ostrom (2010).

[64]Crawford and Ostrom (2005), p. 137.

[65]Ostrom (2010), p. 651.

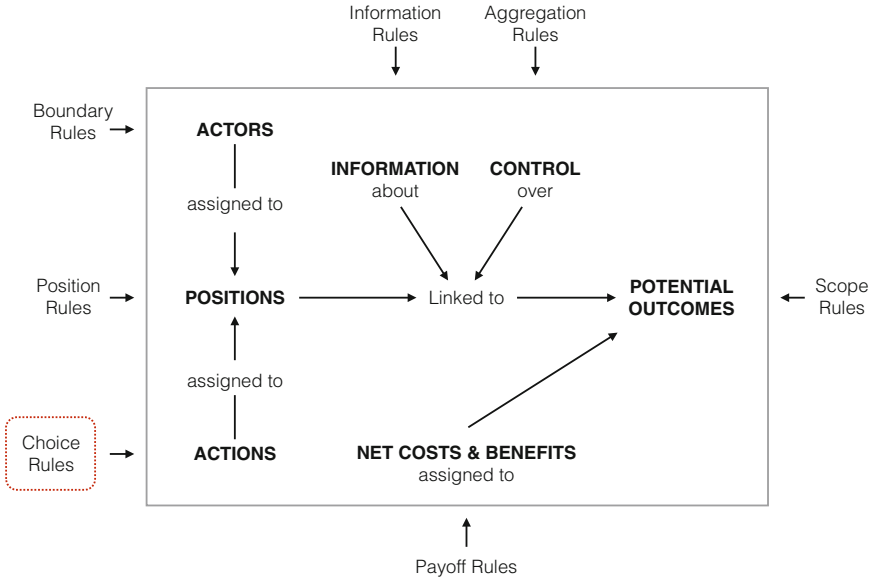

Fig. 4 Rules as exogenous variables directly affecting the elements of an action situation (Ostrom 2010, p. 651)

entry and defining the position of actors are of great significance as well (e.g., situation where employee inventors are willing to become independent entrepreneurs especially if the employer shows little interest in commercializing employee invention). Hence, boundary and position rules should not be too rigid and enable the employee quickly change the status from company employee to an independent entrepreneur. Similar flexibility is desirable when it comes to rules governing choices and payoffs. Various examples about possibility to increase the possibilities to choose actions and modes of payoffs could be inferred from joint R&D projects. Parties' agreement as to the allocation of ownership rights to newly developed products should be in principle upheld (e.g., who obtains rights to register patents to a newly developed technology, sharing the burden of maintenance of IP rights, rights of inventors, etc.). If dissemination of information and growth are understood as the main goals innovation ecosystem, then choice rules should be employed to perform the catalyst function for generation of disruptive business models.

6 Conclusion

This chapter aimed to facilitate the debate about the role of social capital and mutual trust in facilitating creativity and innovation. We saw that although IPRs and rules on competition play an important role in stifling innovation, some

other factors such as mutual trust play a no less important role in facilitating the exchange of information and reducing transaction costs. Moreover, a social capital perspective offers a fresh approach to reconsider prevailing justifications of IP rights system. This chapter also submits that the one of the main innovation policy goals should be facilitation of information dissemination. In order to attain that objective, it is desirable to offer various incentives to increase the number of competing intermediaries. It was also emphasized that creativity and innovations could flourish if the amount of social capital is greater. From a legal point of view, this could be done by flexibly interpreting and applying legal rules so that the choices generated by the creators could be legally recognized.

References

Bentham J (1996) Introduction to the principles of morals and legislation. Oxford University Press, Oxford

Balganesh S (2013) The uneasy case against copyright trolls. South Calif Law Rev 96:723

Bessen J, Meurer MJ (2008) Patent failure: how judges, bureaucrats and lawyers put innovators at risk. Princeton University Press, New Jersey

Burstein MJ (2012) Exchanging information without intellectual property. Tex Law Rev 91:230

Benkler Y (2006) The wealth of networks: how social production transforms markets and freedom. Yale University Press, New Haven

Bock L (2015) Work rules! Insights from inside Google that will transform how you live and lead. Twelve, New York

Bowles S, Gintis H (2002) Social capital and community governance. Econ J 112:F419

Burt RS (2004) Structural holes and good ideas. Am J Sociol 110:349

Castelfranchi C, Falcone R (2010) Trust theory: a socio-cognitive and computational model. Wiley, Singapore

Chen Y (2014) Refusal to deal, intellectual property rights, and antitrust. J Law Econ Organ 30(3): 533

Chesbrough H, Vanhaverbeke W, West J (2006) Open innovation: researching a new paradigm. Oxford University Press, Oxford

Coase R (1937) The nature of the firm. Economica 4:386

Coase R (1960) The problem of social cost. J Law Econ 3:1

Coleman JS (1988) Social capital and the creation of human capital. Am J Sociol 43:95

Coleman JS (1990) Foundations of social theory. Harvard University Press, Cambridge

Crawford SES, Ostrom E (2005) A grammar of institutions. In: Ostrom E (ed) Understanding institutional diversity. Princeton University Press, New Jersey

Damstedt BG (2003) Limiting locke: a natural law justification for the fair use doctrine. Yale Law J 112:1179

Dasgupta P (2005) Economics of social capital. Econ Rec 81:2

Dasgupta P, Serageldin I (2000) Social capital: a multifaceted perspective. World Bank, Washington D.C.

Fisher WW (2004) Promises to keep: technology, law, and the future of entertainment. Stanford University Press, Stanford

Gambetta D (1988) Can we trust trust? In: Ganbetta D (ed) Trust: making and breaking cooperative relations. Basil Blackwell, Cambridge

Gervais D (2012) Challenges in intellectual property governance: providing the right incentives in the quest for global innovation. Trade Law Dev 4:385

Granovetter M (1973) The strength of weak ties. Am J Sociol 78:1360

Hwang VW, Horowitt G (2012) The rainforest: the secret to building the next Silicon Valley. Regenwald, Los Altos Hills
Hardin R (2002) Trust and trustworthiness. Russel Sage Foundation, New York
Hughes J (1988) The philosophy of intellectual property. Georget Law J 77:287
Kleiberg J et al (2009) Strategic network formation and structural holes. goo.gl/ZwqTgs. Accessed 1 Oct 2016
Landes WM, Posner R (2003) Economic structure of intellectual property law. President and Fellows of Harvard College, Cambridge
Lessig L (1999) Code and other laws of cyberspace. Basic Books, New York
Levi M (2003) The transformation of a skeptic: what nonexperimentalists can learn from experimentalists. In: Ostrom E, Walker J (eds) Trust and reciprocity: interdisciplinary lessons for experimental research. Russell Sage Foundation, New York
Lieberman M (2014) First mover advantage. In: Augier M, Teece DJ (eds) Palgrave encyclopedia of strategic management. Palgrave, New York
Lin N (2001) Social capital: a theory of social structure and action. Cambridge University Press, Cambridge
Lobel O (2013) Talent wants to be free. Yale University Press, New Haven
Locke J (2010) Second treatise of government. Infomotions, South Bend
Luhmann N (1979) Trust and power. Wiley, Chichester
Luhmann N (2000) Familiarity, confidence, trust: problems and alternatives. In: Gambetta D (ed) Trust: making and breaking cooperative relations. Blackwell, New York
McGowan D (2004) Copyright nonconsequentialism. Mo Law Rev 69:1
Mayer RC, Davis JH, Schoorman FD (1995) An integrative model of organisational trust. Acad Manag Rev 20:709
McCahery JA, Vermeulen E (2014) Ignored "Third" dimension of corporate governance. https://goo.gl/qrdKYf. Accessed 1 Oct 2016
Merges RP (2007) Locke for the masses: property rights and products for collective creativity. Hofstra Law Rev 36:1179
Merges RP (2011) Justifying Intellectual Property. Harvard University Press, Cambridge
Mill JS (1998) Principles of political economy. Oxford University Press, Oxford
Mossoff A (2012) Saving locke from Marx: the labor theory of value in intellectual property theory. Soc Philos Policy 29:283
Nahapiet J, Ghoshal S (1998) Social capital, intellectual capital and the organizational advantage. Acad Manag Rev 23:242
Ostrom E, Ahn TK (2003) Introduction. In: Ostrom E, Ahn TK (eds) Foundations of social capital. Edward Elgar Publishing, Cheltenham
Ostrom E (2005) Understanding institutional diversity. Princeton University Press, Princeton
Ostrom E (2010) Beyond markets and states: polycentric governance of complex economic systems. Am Econ Rev 100:641
Putnam R (1994) Making democracy work: civic traditions in modern Italy. Princeton University Press, Princeton
Rigamonti CP (2006) Deconstructing moral rights. Harvard International Law Journal 47:353
Silbey J (2014) The Eureka myth: creators, innovators, and everyday intellectual property. Stanford University Press, Stanford
Solomon RC, Flores F (2003) Building trust: in business, politics, relationships, and life. Oxford University Press, Oxford
Suarez F, Lanzolla G (2005) The half-truth of the first mover advantage. Harv Bus Rev. https://goo.gl/bb8FqT. Accessed 1 Oct 2016
Sztompka P (1999) Trust: a sociological theory. Cambridge University Press, Cambridge
Schmidt E, Rosenberg J (2015) How Google works. Grand Central Publishing, New York
Teramoto S, Jurčys P (2014) Innovation, trust and efficiency of communication: a social network perspective. In: Fenwick M, Van Uytsel S, Wrbka S (eds) Networked governance, transnational business and the law. Springer, Dordrecht

Teramoto S, Larasati D, Jurčys P (2014) Diversity of distributed music and modern telecommunication technologies: a network perspective. Kyushu University Legal Research Bulletin 4. http://goo.gl/MCWW5A. Accessed 1 Oct 2016
Tuomela R (1993) What is cooperation. Erkenntnis 38:87
Vickers J (2010) Competition policy and property rights. Econ J 120:375
Williamson OE (1983) Markets and hierarchies: analysis and antitrust implications. Free Press, New York
Williamson OE (1993) Calculativeness, trust, and economic organisation. J Law Econ 36:45
Williamson OE (1998) Economic institutions of capitalism. Free Press, New York
Williamson OE (2010) Transaction cost economics: the natural progression. Am Econ Rev 100:673
Zemer L (2006) The making of a new copyright lockean. Harv J Law Public Policy 29:89
Zittrain J (2008) The future of the internet and how to stop it. Yale University, New Haven

Nudging Cloud Providers: Improving Cloud Architectures Through Intermediary Services

Marcelo Corrales and George Kousiouris

Abstract Two of the most important developments of this new century are the emergence of Cloud computing and Big Data. However, the uncertainties surrounding the failure of Cloud service providers to clearly assert "ownership" rights of data during Cloud computing transactions and Big Data services have been perceived as imposing transaction costs and slowing down the capacity of the Internet market to thrive. "Click-through" agreements drafted on a "take it or leave it" basis govern the current state of the art and they do not allow much room for negotiation. The novel contribution of this chapter proffers a new contractual model advocating the extension of the negotiation capabilities of Cloud customers, enabling thus an automated and machine-readable framework, orchestrated by a "Cloud broker." Cloud computing and Big Data are constantly evolving and transforming into new paradigms where Cloud brokers are predicted to play a vital role as an intermediary adding extra value to the entire life cycle. This chapter situates the theories of behavioral law and economics ("Nudge Theory") in the context of Cloud computing and Big Data, and takes "ownership" rights of data as a canonical example to represent the problem of collecting and sharing data at the global scale. It does this by highlighting the legal constraints concerning Japan's Personal Information Protection Act (Act No. 57 of 2003, hereinafter "PIPA") and proposes a solution outside the boundaries and limitations of the law. By allowing Cloud brokers to establish themselves in the market as entities coordinating and actively engaging in the negotiation of Service Level Agreements (SLAs), individual customers and Small and Medium-sized Enterprises (SMEs) could efficiently and effortlessly choose a Cloud provider that best suits their needs. This can yield radical new results for the development of the Cloud computing and Big Data market.

M. Corrales (✉)
Institute for Legal Informatics, Leibniz Universität Hannover, Hannover, Germany
e-mail: marcelo.corrales13@gmail.com

G. Kousiouris
Department of Electrical and Computer Engineering, National Technical University of Athens, Athens, Greece

M. Corrales et al. (eds.), *New Technology, Big Data and the Law*,
Perspectives in Law, Business and Innovation, DOI 10.1007/978-981-10-5038-1_7

Keywords Cloud computing · Big Data · "Ownership" rights · Service Level Agreements (SLAs) · Nudges · Choice architectures

Contents

1 Introduction

Perhaps one of the most appropriate metaphors for the Internet is that of an iceberg. The average person recognizes a small fraction visible above the surface, the top 10%.[1] Underneath the waterline, however, are various layers of hidden technology,[2] leaving 90% of the mass largely unseen.[3] This is known as the Internet architecture[4] or computer "code."[5] This chapter is about planning and designing specific features of that hidden architecture using alternative approaches that affect the legal environment for innovation and economic growth. A good reason to focus on the architecture design is that much of the legal literature attempts to influence and amend the law. Most lawyers and legal scholars hardly discuss the implementation of embedding legal concepts into the user interface and related systems. Nevertheless, it is more important to focus, in particular, on shaping the basic technological pillars of the Internet and injecting legal requirements into their implementation. Surely, that would represent a more effective and practical approach.[6]

[1]Muller (2015), p. 168.
[2]Horten (2016), p. 135.
[3]Lightman (2002), Preface.
[4]See, e.g., Van Schewick (2010), pp. 1–586.
[5]Lessig (1999), pp. 1–320; Reidenberg (1998), pp. 553–593.
[6]See, e.g., Bygrave and Bing (2009), pp. 3–4.

This chapter attempts to analyze these issues by examining recent theories within behavioral law and economics, which are steadily on the rise and increasingly relevant as a point of reference in policy-making and regulation. In this regard, behavioral economics offers a normative framework that can help us better understand the pitfalls of any decision-making process. The specific goal is to advance a fresh approach to the economic analysis of contract law in Cloud computing transactions that is based on a more reliable and accurate understanding of choice and human behavior. It attempts to build on early driven theories of behavioral economics and outline a framework addressing the potential applications of behavioral insights. The unifying idea of this interdisciplinary analysis is to integrate the tools of traditional law and economics, but taking human behavior for granted with more accurate assumptions and remedies about law.[7] In doing so, this chapter situates the theories of behavioral law and economics in the context of Cloud computing and Big Data, and it takes Japan's PIPA[8] as a canonical example to represent the problem of clarifying "ownership" rights of data in Cloud computing and Big Data scenarios. Overall, it aims to provide a contribution to bridge the gap between end-users (consumers) and Cloud providers through intermediary services.

This chapter is divided into 10 sections. After this introduction, Sect. 2 examines some of the technical and conceptual issues that are useful for the discussion of this study. The purpose of Sect. 3 is to lay the foundations for understanding the legal principles of PIPA, the reasons for its implementation and what context it is currently operating in. By and large, this section is dedicated to providing an insight into the linkage between Cloud computing, Big Data and PIPA by referring to the Suica Card Incident, which created concerns among customers of a railway company in Japan. Section 4 is about Cloud architectures, freedom of choice, and the legitimate scope of Cloud computing brokers in softly nudging end-users and Cloud providers—as a new form of soft paternalism—that can help them to make better decisions without coercing or neglecting their choices. Section 5 outlines how we can turn certain nudging techniques into simpler and more effective SLAs. Section 6 explains how default rules, warnings and information disclosure can help end-users to improve decision-making when choosing a Cloud provider. Section 7 explains the new contractual framework from a high-level perspective and Sect. 8 goes into more details with regard to the automated process. Section 9 explains how this framework has been embedded into a software toolkit that is readily available for downloading from the Internet. Finally, Sect. 10 concludes with a contractual framework that has been encapsulated in a new paradigm with a more purposive and Cloud-market-oriented approach.

[7]See, e.g., Jolls, Sunstein and Thaler (1998), pp. 1471–1550.

[8]Personal Information Protection Act (No. 57 of 2003).

2 Cloud Computing and Big Data Sprawling the IT Market

Two distinct—but at the same time closely related—emerging technologies stand out from the kernel of this research: Cloud computing and Big Data. While Cloud computing is not a new technology it is a new way of providing on demand services that is continually and rapidly evolving into different business models.[9] The last decade has witnessed the burgeoning of the Cloud computing market, which lead to an increase in the number of Cloud services at the international level. The Cloud shifted[10] the way computing services are managed today,[11] offering many advantages to business[12] and scientific research.[13]

Part of the reason is that IT resources in the Cloud are not locally stored on end-user personal devices[14] but accessed through a distributed network. This enables consumers to operate a broad spectrum of applications ranging from email and spreadsheets to more robust and reliable business software.[15] This paradigm was inspired from the central idea that computing will become a public utility, just like water, gas and electricity.[16] Cloud computing has become a widespread tool that is constantly evolving into new ways of providing services, which are present in almost every transaction that we make in our daily lives. Studies reveal that the Internet will take on a "brokerage form" in all fields, especially among Cloud ecosystems. Cloud brokers could aid in the provision of new services that enable flexibility, interoperability, scalability and highly secured technologies compatible with the Cloud computing models popular today on the Internet.[17]

Big Data is also sprawling the IT landscape and needs Cloud computing power to process massive amounts of data.[18] It relies on the distributed storage of Cloud services as the underlying infrastructure for smooth operation. Although there are many overlapping concepts and technologies in Cloud computing and Big Data, they differ in the following major aspect: Cloud computing transforms directly the IT architecture, whereas Big Data operates in the upper level and influences the analyses in science and business decision-making process.[19] Both Cloud computing

[9]Murugesan and Ananth (2016), p. 4.
[10]Balasubramanyam (2013), p. 102.
[11]Srinivasan (2014), p. 5.
[12]Millham (2012), p. 2.
[13]Catlett et al. (2013), Preface.
[14]Kasemsap (2015), p. 31.
[15]Biswas (2014), p. 333.
[16]Marinescu (2013), Preface.
[17]Murherjee and Loganathan (2014), pp. 142–143.
[18]Kannan et al. (2016), Preface.
[19]Chen et al. (2014), pp. 12–13.

and Big Data complement each other, and are, therefore, the ideal combination that may very well disrupt the world.[20]

Big Data is usually collected from different sources and is presented in a raw state. Much of this information is generated in wholly transnational settings. The premise is to gather as much data as possible, then analyze it by using data mining tools, artificial intelligence and analytic tools from servers that can be located in different places. This data is then curated and categorized in various ways to find the answers for everyday problems. Therefore, Big Data can be viewed as a set of information processing tools and methods, which open new possibilities for the analysis and use of massive amounts of data.[21]

Taking advantage of the benefits of Big Data seems essential. Nevertheless, from the perspective of law and organizations, Big Data creates a new and difficult set of questions, which requires a re-thinking of the existing legal rules covering IT matters. More generally, technology has developed so rapidly that current regulatory and policy approaches face severe difficulties and limitations just keeping pace with on-going technological disruption. This problem has been compounded by the degree of interaction between societies, and the social reality that data can now be transferred across borders. This situation is particularly complex because the global nature of Cloud computing and Big Data raises a new set of difficult legal issues. To be sure, much of the contemporary legal debate has revolved around questions of privacy and data protection.[22]

3 The Suica Scandal and a New Legal Landscape for Big Data in Japan: Who "Owns" the Data?

Japan's PIPA is one of the oldest laws in Asia regulating privacy and data protection. Over recent years, a number of cases related to data security breaches and unlawful sales of personal data have occurred.[23] The Japan Railway "Suica Card Incident" is probably the most well-known such incident. The East Japan Railway (JR East) decided to sell travel records information of its prepaid Suica Cards to a third-party company (Hitachi) without the prior consent of its 43 million customers. The Suica Card is a rechargeable train pass that can also be used to purchase goods in a range of stores. When the incident came to public attention, the railway company claimed that this was "anonymized" data and "statistical information," which did not violate any data protection laws. JR East publically apologized for the incident and offered its customers the opportunity to opt-out of the data

[20]Mosco (2014), pp. 1–284.

[21]Adhikari and Adhikari (2015), pp. 4–5; Chen et al. (2014), p. 12.

[22]Corrales and Jurčys (2016).

[23]Parsons and Colegate (2015).

collection scheme by sending an e-mail.[24] Nevertheless, a number of customers claimed that the advanced analytic tools of private marketing companies would make it possible to identify patterns in the "anonymous" data and, in this way, had the potential to establish links to customers' commuting and other purchasing behavior.[25] Furthermore, there was the possibility of data triangulation, meaning that a combination of two apparently anonymized sources together, could allow the extraction of personal identifiers.[26] Although it is unclear whether JR East violated PIPA, this incident fuelled anxiety among Japanese consumers regarding data security. Moreover, this case raised public awareness of the need to have a more clear set of rules regarding data management.[27] As a result, JR East received a number of complaints from customers and terminated its contract with Hitachi.[28]

Against this background, a series of amendments have been made to PIPA. While some of the changes came into effect from 1 January 2016, other changes are expected to enter into force by September 2017. Among the most significant changes, four of them deserve attention in the context of a discussion of Big Data and the Internet.[29] First, the revised PIPA contains specific rules for the transfer of personal data to third countries and international organizations. This change is designed to ensure an adequate level of protection in a globally connected society. Second, these new provisions increase the responsibilities of data controllers and place new constraints on the export of personal data from Japan to overseas countries. Third, the amendments expanded the scope of the definition of "sensitive personal information" and created clear restrictions regarding biometric data such as fingerprints, face recognition, as well as any personal numeric identification codes. Finally, the revised law sets up a regime that takes into account the Big Data movement. "Anonymized" data can now be sold to third party companies for marketing purposes, subject to certain limitations. For instance, PIPA requires data controllers to maintain comprehensive and accurate records of data in reasonable detail. In addition, the disclosure of Big Data must be reported to the competent authority and communicated to the public.[30]

Aside from these changes in the framework of the substantive law, Japan has made several institutional changes to strengthen the data protection regime. The most important change has been the establishment of a new central government agency, the Personal Information Protection Commission (PIPC). The PIPC replaced the former Specific Personal Information Protection Commission, and operates as an independent administrative agency. One of the key objectives of PIPC will be to ensure that personal data is processed lawfully when transferred to

[24]Metcalfe (2013).

[25]The Japan Times (2013).

[26]Béranger (2016), p. 85.

[27]Crawford (2015).

[28]Mainichi Japan (2015); see also Corrales and Jurčys (2016).

[29]Corrales and Jurčys (2016).

[30]Amended Act on the Protection of Personal Information (2016); see also Winston & Strown LLP (2015), Corrales and Jurčys (2016).

third countries.[31] For example, Article 24 of the revised PIPA imposes limitations on the transfer of personal information of Japanese citizens to foreign countries (defined as any country or territory outside of the region of Japan), excluding those countries deemed to possess personal information protection systems that are recognized to be at the same level as Japan's, in terms of protecting individual rights and interests. This can be seen as an attempt to move the Japanese regulatory framework closer to the EU General Data Protection Regulation. Moreover, these legislative steps can serve as a model for other Asian countries and contribute to harmonization at the regional level.[32]

Nevertheless, despite modifications in the legal and institutional framework, the government is not discussing issues with respect to general consumers. The discussion concerning "ownership" rights of data is inherently related to the concept of respect with regard to the origin and source of the data. The legal discussion of data protection, non-disclosure of information and the confidentiality of data are not enough. The implementation of the concept of respect in the regulation or even at a contractual level seems to be very difficult. However, the practical implementation of this concept embedded into the user interface or user experience seems to be more feasible.

The nature of this concept can be gleaned from the experience of how to establish informed consent in the medical field. Informed consent and decision-making is an ongoing process. It is a continuous effort to ensure meaningful communication and respect to patient's autonomy.[33] Embracing this concept could also help to build more trusting relationships. Most legal scholars tend to cluster towards conventional concepts and normative approaches related to database rights, privacy, data protection and security. However, we have to strike a balance between integrity, availability and confidentiality. Within the scope of Big Data, when a service company is collecting data, Big Data does not solely belong to the connecting company. The company is a fiduciary and, as such, it has fiduciary obligations to the beneficiaries whose data is held in their databases.[34]

The situation is daunting, to put it mildly. It could be said that due to its global nature, the Cloud is riddled with all sorts of legal concerns. Much of this legal debate has been focused on solving data protection and data security issues whereas Intellectual Property Rights (IPRs) have fallen behind schedule. The difficulty is that the conventional focus of IPRs has been structured in such a way as to exclude

[31]See Personal Information Protection Commission.

[32]Corrales and Jurčys (2016). Furthermore, proposals for standardizing contractual model terms like in the case of the SLALOM project may aid towards this direction, given that standardization is inherently an international effort that requires consensus and can achieve interoperability of regulatory and technical frameworks. See generally, Rinaldi and Stella (2016). The SLALOM Project is co-funded by the European Commission through the H2020 Program under Grant Agreement 644720.

[33]For a comprehensive view on respect to patient's autonomy and informed consent in the medical field see Maclean (2009), p. 42; see also generally, Veatch (1997), pp. 195 et seq.

[34]About fiduciary responsibilities of Big Data see, e.g., Berman (2013), pp. 201–211.

others from creating potential solutions. In the authors view, the actors involved in IPRs need a new approach to protect their information. In this research, it was decided to focus on the question of "ownership" rights of data because there is a significant gap in the literature that has been overlooked by legal scholars in the field. Clarifying who "owns" such data on the Internet has been one of the main bottlenecks for the Cloud market.[35] This means that we need a new framework for understanding, protecting and sharing large sets of data. A framework that is more flexible and serves as an instrument for coordination and choice.

The growing outward orientation of the law until now has shown no agreement towards a global standard that defines "ownership" rights of data. At the outset, it is important to consider this general observation and the absence of a legal terminology to interpret this term more accurately. In the title of this section, and throughout this chapter, the word "ownership" has been intentionally quoted. In so far as it refers to data, the concept of "ownership" is not a legal construct. This notion has been borrowed from the sphere of tangible property and is used as an analogy, which is extended to intangible rights such as data or information. This concept glosses over various issues and it is far from being clear or correct. It could be said that it falls in some sort of twilight zone where neither domestic laws nor international treaties can really shed light on this point. They are in a "grey area"; somewhere between the traditional protection granted by IPRs and tangible rights. Thus, "ownership" rights of data will be treated here as synonymous with the concept of "owning" information, roughly homogenous to property rights[36] in physical form. Although not without certain difficulties, this generalization, is adequate as enough similarities exist to justify and admit this stylization for present purposes.

4 A Behavioral Law and Economics Approach

As a body of learning, the field of behavioral economics is as old as the discipline of law and economics itself. The marrying of psychology and economics can be traced back to 1958 and emerged as an independent "bona fide" sub-discipline of economics.[37] This field analyzes a variety of psychological, emotional,[38] social and cognitive factors that induce economic decision-making.[39] It became apparent very

[35]See, e.g., Al-Khouri (2012), pp. 1–8.

[36]Property rights can be categorized in different ways, most of which fall outside the scope of this chapter. Generally, this term can be broken down in two main areas: (a) *corporeal*: covering items which relate to an object, a thing. Something tangible that is a physical good e.g., a car, a computer; (b) *incorporeal*: covering items that are not visible to human eye. Something virtual and intangible by nature, e.g., data, information. See Robson and McCowan (1998), p. 15; Corrales et al. (2010), pp. 293–294; Elkin-Koren and Salzberger (2013), p. 44.

[37]Angner and Loewenstein (2016).

[38]See generally, Zeiller and Teitelbaum (2015).

[39]See generally, Minton and Kahle (2013), pp. 1–149.

early that this discipline needed to be united with the law to be able to manage firms effectively or to influence public policy and economic decision-making. This field called *behavioral* law and economics blends insights from cognitive psychology and economy as the overarching framework to discuss legal issues. Behavioral law and economics' fundamental premise stems from an innate human propensity to "err" in making decisions.[40]

The idea to incorporate the findings of behavioral and social sciences in shaping the law and government policies has now entered the mainstream of modern law and economics and became increasingly popular in the works of Richard Thaler and Cass Sunstein. They have argued that improved choices, default rules and information disclosure could softly nudge citizens to make better decisions, improve welfare and enhance the efficiency of government.[41] According to the 2015 World Development Report: "The promise of this approach to decision making and behavior is enormous, and its scope of application is extremely wide…Research shows that small differences in context, convenience, and salience have large effects on crucial choices…"[42] According to an article published by The Economist: "this body of work is best understood as a set of exceptions that modifies but leaves intact the canonical model of rational choice, not least since it is irrational to suppose that people in general behave irrationally."[43]

On this type of account, behavioral economists are not suggesting that individuals behave irrationally. On the contrary, they concur with the idea that individuals are fully rationals, but sometimes they may blunder due to certain systemic limitations in that rationality. The stimulus for, and central idea of, behavioral economics in law is to take this "bounded rationality" into account in designing any regulatory scheme.[44]

Herbert Simon coined the term "bounded rationality" and it means simply that there are some "boundaries" to any rationality.[45] He used the metaphor of

[40]Jolls et al. (1998), pp. 1471–1550.

[41]In the UK for instance, the Prime Minister David Cameron established a "Behavioral Insights Team" in the Cabinet Office with the specific objective of including the psychological analysis of human behaviour into policy-making initiatives in various areas such as anti-smoking, energy efficiency, consumer protection, organ donation, etc. See Behavioral Insights Team; see also Wright (2014). In the United States, the Obama administration created a team in 2013 in order to do empirical research of behavioral sciences. Recently, in September 2015, President Obama signed an executive order, which encourages federal government agencies to use behavioral science insights to better understand and serve the American people. See Executive Order—Using Behavioral Science Insights to Better Serve the American People, The White House, Office of the Press Secretary (2015).

[42]World Bank Development Report (2015).

[43]The Economist (2006).

[44]See, e.g., generally, Munro (2009).

[45]Simon (1972), p. 162; see also generally, Pomerol (2012), pp. 70–71; Lathi (2010), p. 35; Simon (1998), pp. 270–274.

scissor's[46] to explain the interaction between cognitive strategies and the structure of environmental context.[47] He suggested that there is a dual limitation process that individuals face while making a decision. One blade of the scissor being the cognitive bias and the other the environmental constraints such as finite amount of time, lack of information[48] and resources available.[49] Contrary to the prevailing approach in traditional economics, it has been recently more widely acknowledged that individuals do not behave as perfectly rational actors. There are obvious boundaries to one's own willpower and self-control.[50]

More recently, behavioral scientists have also shown that individuals often tend to act unselfishly and may be too optimistic. This is because they rely on the limited resources available to perceive and process information more accurately by virtue of the abovementioned mental shortcuts known as "heuristics and biases." The technical definition of heuristic is: "a simple procedure that helps find adequate, though often imperfect, answers to difficult questions."[51] In this case, the heuristic question is: "the simpler question that you answer instead."[52] This being said, behavioral law and economics may offer us some new insights or certain cues for legal reform.[53] This approach provides more structured choices without restricting or neglecting individual's right to choose than can lead to more positive outcomes. Richard Thaler, Cass Sunstein and others, have focused on these psychological traits of human behavior, which may offer perhaps a more realistic foundation to law and economics.[54]

This movement is also known as "libertarian paternalism." This concept combines two ideas that seem to contradict each other. The libertarian aspect lies in the general principle that people know what is good for them and therefore should be free to do whatever they want to do. Whereas the idea of paternalism "attempts to influence the choices of affected parties in a way that will make choosers better off."[55] According to Thaler and Sunstein, this idea however is not an "oxymoron," but both possible and totally legitimate for private and public institutions to influence decision-making without coercion. This is also called "soft paternalism"

[46]As Herbert Simon pointed out: "Human rational behavior (and the rational behavior of all physical symbol systems) is shaped by a scissors whose two blades are the structure of task environments and the computational capabilities of the actor." See Simon (1990), p. 7.

[47]Clark et al. (2012), Preface; Reb et al. (2014), p. 14; Gigerenzer (2000), p. 125.

[48]Gigerenzer and Selten (2002), p. 4; see also generally, Simon (1955), pp. 99–118; Simon (1984), pp. 1–392.

[49]Viale (2012), p. 25.

[50]Connolly and Coburn (2016), p. 41.

[51]Kahneman (2011), p. 98.

[52]Kahneman (2011), pp. 97–98. The etymology of the word "heuristics" comes from Greek "*heureka*," which literally means, "I have found (it)" from the verb "*heuriskein*" (to find). This expression became famous as it was supposed to be shouted by Archimedes (c. 287–212 B.C.E.) when he found the solution to a scientific problem. See Online Etymology Dictionary; Utts (2014), p. 348.

[53]See, e.g., Sunstein (2000).

[54]Heukelom (2014), Introduction, pp. 1–10, 168.

[55]See Thaler and Sunstein (2003), pp. 1–3.

because it respects freedom of choice, while at the same time it attempts to guide people's choices towards the promotion of welfare. Thaler and Sunstein themselves are key figures in this movement.[56]

The underlying basis of this approach is substantiated in empirical research carried out by psychologist Daniel Kahneman, notably in *Thinking, Fast and Slow*. In this book, he develops an account of human psychology based on the idea that we all have two ways of thinking: "thinking fast" (System 1) and "thinking slow" (System 2).[57] Whereas the former is emotional, impulsive and difficult to control, the latter is reflexive, measured and more amenable to external influence. Individuals tend to use System 1 and substitute difficult questions (e.g., issues of a legal or technical nature) for an easier one. This works as a kind of mental shortcut that, every so often, may result in errors.[58]

For Kahneman, the human brain operates as if there are two different fictitious characters, each with different capacities, attributes and personalities. It does this since this is the most efficient way for the human brain to process and acquire information. System 1 operates automatically and effortlessly, and—most of the time—it is the one that we use, without being fully conscious of the processes involved in such decision-making. It is extremely fast and perceptive.[59] For instance, when somebody asks you to name the capital of Germany, the answer comes to mind instantly, or when someone asks you what is 2 + 2? The result comes in a split-second and without deliberate or conscious thinking. The other agent (System 2) is slower, more flexible and involves conscious monitoring. It has two functions: one of them is to compute more difficult tasks such as finding the results of complex arithmetic. In such a case, the answer does not come immediately, as in the previous 2 + 2 example. A more difficult calculation requires the expenditure of some time and effort in order to find the result. Another function of System 2 is to monitor the behavior of the mind. The main characteristic of this mode is that individuals need to exert some effort in order to find a solution.[60]

---

[56]Thaler and Sunstein (2003), pp. 1–3; but see White (2013), pp. 1–185. White argues generally against the idea of paternalistic nudges by the government and makes a positive claim in favor of individual choice and autonomy.

[57]The terms System 1 and System 2 were first coined by Stanovich and West and will be used along this chapter. See Stanovich and West (2000), pp. 645–665.

[58]Kahneman (2003), p. 698.

[59]Kahneman (2003), p. 698.

[60]Kahneman (2003), p. 698; Kahneman (2011), pp. 20–26; see also Stanovich (2010). In this book, Stanovich established the difference between rationality and intelligence and suggests that some individuals are closer to System 1 and some others are closer to System 2. He also established a distinction of two parts of System 2, what he calls "two separate minds." According to him, System 2 has a dual-process and must be divided into the "reflective mind" and the "algorithmic mind." According to Stanovich's concept, superficial or "lazy" thinking is a flaw in the reflective mind, and explains how individuals can behave sometimes irrationally. See also Kahneman (2011), pp. 48–49. In evolutionary terms, System 1 is older than System 2. It relates to our animal instincts and is broken down in a subset of systems that include both our innate abilities and "domain-specific knowledge" learnt from a "domain-general learning" system. System 2 is

Being aware of these two types of mental operations goes hand in hand with the systematic framework of this research. System 1 focuses on how the information is presented, it relies on shortcuts and illusions, whereas System 2 overturns present biases and heuristics, detects errors and recognizes omissions. Constant developments and changes taking place in the field of information and communication technology, especially in the area of Cloud computing and Big Data, has posed serious challenges and threats to employees and management teams. Advances in technology are happening so fast that it is difficult for them to assess how to collect, store, and process data for competitive advantages.[61] It is therefore even more overwhelming to choose the right Cloud provider. An additional way businesses and organizations can leverage Cloud computing and prevent these heuristics and biases is through the experience and technical expertise of Cloud brokers. End-users and companies can make faster and better decisions by bringing intermediary services involved in these processes. The following sections cover a variety of techniques to overcome these heuristics and biases that can help to make better decisions for companies and organizations.

4.1 Nudge Theory and Cloud Brokerage Architectures

Nudge theory mainly operates by "designing" or "re-shaping" choices that influence and encourage individuals and society to improve and enforce decision-making provided by the government, companies and other authorities.[62] Choice architectures are present from the very moment that we use the law to try to influence society. This includes the idea of nudges. The Collins dictionary definition of a nudge is "to push or poke (someone) gently…to give (someone) a gentle reminder or encouragement."[63] Similarly, the Oxford dictionary defines nudge as to "prod (someone) gently, typically with one's elbow, in order to draw their attention to something," or simply "to touch or push (something) gently or gradually."[64]

For Thaler and Sunstein, a nudge refers to "any aspect of the choice architecture that alters people's behavior in a predictable way without forbidding any options or significantly changing their economic incentives."[65] Or, put in more simple terms, a nudge is "every small feature in the environment that attracts our attention and

(Footnote 60 continued)

more recent and belongs only to humans. It allows abstract and hypothetical ways of reasoning and thinking. It is linked to language and intelligence but is limited in memory capacity. See Evans (2003), pp. 454–459.

[61]Raisinghani (2015), p. 188.

[62]Businessballs.com (Nudge Theory).

[63]See English Collins Dictionary (Nudge).

[64]See Oxford Dictionary (Nudge).

[65]Thaler and Sunstein (2009), p. 6.

influences the decision that we make."[66] Nudges can be very helpful for individuals and society. Some of these nudges may be regarded to be more controversial than others. For example, road signs are undeniably helpful for the community thus they can be regarded as less controversial unless they are misplaced. If so, they could be distracting and may lead to accidents. Otherwise, they generally provide good references and warn road users to drive more carefully.[67]

Thaler and Sunstein mention a good example of a visual 3D illusion painted on the road close to a curve in Chicago's Lake Shore Drive. The painting resembles a speed bump that nudges drivers to tap their brakes and slow down. This illusion creates the same effect of a real bump that uses vertical deflection. The advantages of using this road illusion are manifold: (i) it cost only $500 instead of $2000, (ii) there is no danger for ambulances and similar emergency vehicles, and; (iii) it avoids water floods.[68] The 3D illusion and road sign examples are put in place by someone called a "choice architect," i.e., someone who has "the responsibility for organizing the context in which people make decisions."[69] This is also evident in the case of a cafeteria or a restaurant, where someone has to decide where to locate the salad bar, the bread or the coffee. That person is also a "choice architect" because the way in which she arranges the food and drinks will influence the choices and actions of customers. If the choice architect places the salad bar at the entrance and within a visible range, it is most likely that the customers will take the salad first as a healthier choice.[70] This highlights an important point. Sometimes individuals need a nudge to make better decisions.[71] In this context, the definition of architecture seems to be broad and goes beyond the physical space of the restaurant. As in the lead-off Daily Grill restaurant example, Sunstein explains how the healthier Simply 600 (calories) menu is also a form of architecture. This means that every restaurant, including its menus, contain multiple-choice architectures.

Why Nudge? The Politics of Libertarian Paternalism[72] (Why Nudge) is a more recent work in which Sunstein aims to offer a new approach to the role of government and his libertarian paternalism approach. In this book, he shares his experience working as an Administrator at the White House Office of Information and Regulatory Affairs (OIRA) and discusses various empirical studies conducted, in that context, by cognitive psychologists and economists. Why Nudge develops the argument originally found in *Nudge: Improving Decisions About Health, Wealth, and Happiness*—co-authored with Richard Thaler, which sets out the

[66]Willis (2015).

[67]See, e.g., Jamson (2013), p. 298; Avineri (2014); Nudge.org.

[68]Nudges.org (2008).

[69]Thaler and Sunstein (2009), p. 3.

[70]Thaler and Sunstein (2009), p. 1; Sunstein (2014), pp. 12, 25, 91 and 164.

[71]Behavioral Economics is expanding to different fields in addition to law. See, e.g., Heshmat (2011), Introduction. In addition, nudging techniques can also be used to negatively influence and biase decision-making. The ways many surveys, polls and referendums are framed are all very good examples of this.

[72]Sunstein (2014), pp. 1–221.

principles of how people often and persistently make "poor" choices that run counter to their best interests, at least when viewed from a long-term perspective.

This book focused on choice architecture and opened with one of the most humorous and powerful real-world illustrations of a nudge in bathroom urinals at Amsterdam Schiphol airport. It turns out that men are often a bit careless when using the urinal in the men's room. As an experiment in human behavior, they placed a realistic image of a black fly into each urinal just above the drain in order to provide users with a target they would aim at. After this experiment, "spillage" on the men's bathroom floor was considerably reduced by 50–80%. This is an interesting, simple and inexpensive example of a nudge that gives people a gentle "push" in the right direction, reducing cleaning costs and showing how small changes can make a significant (and positive) difference.[73]

In Why Nudge, Sunstein explains what he means by choice architectures and nudges. He uses multiple illustrative and metaphorical examples to discuss the pervasive nature of architecture of this kind. Structured choices are always around us and, often inadvertently, influence the decisions that we make. The story by the late novelist David Wallace, that Sunstein refers to, reflects in metaphorical terms the central idea of choice architectures, which often exists without individuals even recognizing them.

> There are these two young fish swimming along, and they happen to meet an older fish swimming the other way, who nods at them and says, 'Morning, boys, how's the water?' And the two young fish swim on for a bit, and then eventually one of them looks over at the other and goes, 'what the hell is water?'[74]

The sentiment expressed in this quotation, embodies the view that, there is always background architecture in place, by which all individuals are affected even though they do not recognize it. The immediate point of this story, translated into our daily life activities, suggests the ubiquitous nature of the Internet and Cloud architectures that affect the choices we make. The same holds true for cyberspace. This story resembles the iceberg metaphor discussed in the Introduction. The story of the two young fish and the iceberg metaphor suggest that if you are a user of Cloud computing services and if you are engaging with contractual agreements, there is always the equivalent of water in the background, which is affecting the decisions you make, whether you are fully aware or not, just as the fish are swimming in water, whether they recognize it or not.[75]

A choice architecture serves as a material counterpart of the "interface" (e.g., menu, ordering and structure) of different choices that are available for individuals. How these options are listed or represented, or even created in the first place, will influence the quality of the decisions we make. By way of illustration, besides the canonical cafeteria and restaurant examples, there are many other kinds of

[73]Thaler and Sunstein (2009), p. 20; Clark (2010), p. 176; Evans-Pritchard (2013); Sommer (2009); Corrales and Jurčys (2016), p. 533.

[74]Wallace (2008).

[75]Sunstein (2014), p. 25.

architectures and nudges around us such as the default settings of a printer machine (double-sided or single-sided), which can have a large-scale environmental and economic impact. This is another example that shows how small nudges are not trivial and can make a substantial difference in the long term.[76]

The notion of "architecture" obviously varies in different disciplines and there are many concepts provided in the literature. Even in the computer science field there are many definitions available. Therefore, the concept of architecture used here is that of the standard and widely accepted definition given by the Institute of Electrical and Electronics Engineers (IEEE). According to the IEEE ISO Standard 42010, architecture is defined as follows: "the fundamental organization of a system embodied by its components, their relationships to each other and to the environment, and the principles guiding its design and evolution."[77] Bloomberg provides a very broad definition and in his view not only the technology framework but also the people using the system are part of such architecture.[78] In computer jargon, software architecture is a metaphor that resembles the architecture of a building. It has to do with the high-level structure of the software components, where they are located and who uses them according to the defined roles/actors in the system. Each layer of the software structure comprises different component elements and how they are designed to work with other software components.[79] In the context of this research a broad interpretation of the concept of software architecture is used so that SLA specifications can be included within the definition. Software architecture is about making vital choices and decisions regarding the design of the software.[80]

Choice architectures embrace the idea of nudges. They usually consist of disclosures, warnings and default rules. They are inevitable and they are everywhere.[81] "Nudging" provides useful resources that are supposed to enhance an individual's welfare. A meaningful example in policy-making concerns organ donation in Europe. There are some countries where the default rule is not to require individuals to make a donation in the event of their death. In certain countries, however, there is a reverse default mechanism. When one gets a driving license, there is a box to tick offering an opt-out option. The latter default system makes the percentage of organ donations much higher than the previous "opt-in" based system.[82] Another iconic example of a nudge in a rather more technical context is a GPS system. Such systems are designed to show people the best and/or shortest route possible.

[76]Felin (2014), p. 3.

[77]Ramanathan et al. (2009), p. 171; Eppinger and Browning (2012), p. 7; Abraham et al. (2012), p. 116.

[78]See Bloomberg (2013) p. 12.

[79]Clements et al. (2010), p. 19; Perry and Wolf (1992), p. 44.

[80]See, e.g., Jansen and Bosch (2005), pp. 109–120.

[81]Sunstein (2014), pp. 1–30, 179.

[82]Sunstein (2014), pp. 23 and 108; see also generally John et al. (2013), p. 104; Quigley and Stokes (2015), p. 64; Thaler (2009); Hamilton and Zufiaurre (2014), p. 18.

However, individuals still have the freedom to choose another route, and if they do so, there is a risk they will end up getting lost.[83]

In the context of this research, Cloud brokers can be thought of as important choice architects. The notion of a nudge in this context implies the principle to help end-users and Cloud providers to make better choices and to warn them about potential risks and mistakes. Nudging occurs when behaviors are stimulated through "indirect suggestions."[84] The dominant mood in the current debate seems to emphasize, or even amplify, either the "business-to-consumer" relationship, or, the "government-to-citizen" approach. The first refers to how private companies use different nudging techniques to influence consumer-buying behavior such as in advertisement.[85] In the second relationship there is no direct intervention from the government by means of policies, regulations or enforcement,[86] and focuses on to what extent government paternalism may be justified.[87] Either way, these two modalities always target the consumers or citizens directly. It is, however, a slightly new approach that is adopted here. In particular, the framework advocated here involves "indirect nudging" by which Cloud brokers, on the basis of an automated contractual framework, will play a key role in setting the generally applicable nudging techniques. The main argument here is *not* to nudge consumers or citizens directly but to approach *Cloud providers* instead. This new approach could be interpreted as a modified extension of the industry's "choice editing" role[88] that is also strongly related to the Sunstein narrative. The central idea would be to think of Cloud brokers as the key choice architects.

4.2 *Behavioral Market Failures, Different Types of Nudges and Soft Paternalism*

The nudging idea is not new, but justifying them on the basis of a dormant or veiled rationality is. As hinted above in the previous section, it has existed for many decades, especially in the private sector. Marketing agencies have always relied on nudging strategies to capture the attention of consumers in order to influence their behavior and sell their products.[89] The crucial question in Sunstein's narrative seems to boil down to whether the government is legitimately allowed to use these kinds of nudging techniques, as in the organ donation example. Could this be seen

[83]Sunstein (2014), pp. 28, 73, 74, 77 and 149.

[84]Biddle et al. (2015), p. 377.

[85]See, e.g., Dold (2016), p. 50; Blythe (2013), p. 426.

[86]Biddle et al. (2015), p. 377.

[87]See, e.g., Le Grand and New (2015), pp. 1–3; Van Aaken (2015), p. 88.

[88]Abbots and Lavis (2016), p. 155.

[89]Gigerenzer (2015), pp. 361–362.

as a kind of paternalism? This idea is very controversial, as it seems to be in conflict with core liberal values of autonomy and freedom.[90]

A key strand of Sunstein's argument is to challenge John Stuart Mill's so-called "Harm Principle," by showing how, in some instances, people are prone to error and that some paternalistic interventions are needed and justified.[91] The "Harm Principle" suggests that individuals' actions should only be constrained to prevent harm to others. According to Mill's oft-quoted principle, "the only purpose for which power can be rightfully exercised over any member of a civilized community, against his will, is to prevent harm to others."[92] The justifications for the "Harm Principle" are grounded in the principle that individuals know better what is good for them and that governments do not have access to all the necessary information.[93]

This is what Sunstein calls the "Epistemic Argument," which he argues is sometimes wrong. Sunstein questions and challenges this argument by outlining a non-exhaustive list of cognitive circumstances where humans make various systematic and predicable mistakes. This is what he labels as "Behavioral Market Failures" and the existence of such failures provides a justification for the government to step in and correct them.[94] Sunstein also discusses what he calls the "Paternalistic Toolbox," where he distinguishes different types and sizes of paternalism. The key issue is whether public officials are poised to offer a legitimate intervention for citizens to increase welfare. To some extent they should promote the best rational choice by providing the means for improved decision-making. This might not always be possible but it provides a strong argument for the government to intervene, especially in cases of market failure.[95]

Sunstein introduces a number of distinctions. The first distinction relates to "soft," as opposed to "hard" paternalism.[96] In traditional hard paternalism, a "nanny state" employs coercive powers to compel its citizens to do what is in their best interests.[97] Soft paternalism takes the view that government intervention is legitimate and justified only when the person is consciously aware and acts voluntarily.[98] Mill's well-known example of the person who is about to walk across a damaged bridge (the so-called "Bridge Exception"), illustrates this point clearly.[99] Consider

[90]Corrales and Jurčys (2016), pp. 533–536.

[91]Sunstein (2014), p. 28.

[92]Mill (1859), pp. 21–22.

[93]See, e.g., Brown (1972), pp. 133–158; Perry (1988), p. 92; Riley (2015), p. 11; Corrales and Jurčys (2016), pp. 533–536.

[94]For details about "behavioral market failures" and "default rules" see Sunstein (2015), pp. 206 and 218.

[95]Sunstein (2014), pp. 63–72; Corrales and Jurčys (2016), pp. 533–536.

[96]White (2016), p. 26; Prinz (2013), p. 182.

[97]Bishop (2009), p. 296.

[98]Tanner (2007), p. 200; Hartley (2012), p. 70; Angner (2016), p. 264.

[99]See, e.g., Jackson (2006), pp. 68–69.

the case where the government could not communicate the risks of a bridge that is about to collapse as a result of language difference (i.e., the person about to cross the bridge does not speak the local language and can neither read the signs nor understand any warning signals given). In this scenario, the government's use of force to stop her from crossing the bridge would be justified as her liberty consists in doing what she wants, and falling from the bridge is certainly not her desire in this case.[100]

Nonetheless, if such person is fully aware of the danger and notwithstanding wants to commit suicide, then the soft paternalistic view would allow this person to carry on with her will. The hard paternalistic view would justify however the use of force to stop the person from crossing the bridge even if she knows the danger and wants to voluntarily take her own life. This could be interpreted broadly or narrowly. The main difference according to Sunstein would be the ability to influence them without imposing material costs. Nudges would be regarded as soft if they impose zero or very small costs to choosers.

A second main distinction is the distinction between "means paternalism" and "ends paternalism." Here again, the GPS system is a good example of a nudge based on means paternalism. As pointed out earlier, individuals using a GPS have the freedom to choose another route.[101] This is the ideal kind of paternalism that Sunstein tries to promote[102] and this is the kind of nudges that are proposed in this research, as will be explained further below.

5 Turning Nudges into Simpler and More Effective SLAs

The ideas of Kahneman, Thaler, Sunstein and others are germane to SLAs where the involved parties are still free to make a choice. When designing a contract, it is important to follow the nudge theory and apply it correctly to the case. The point is to help both end-users and Cloud providers to make better decisions. How to foster rationality within Cloud computing transactions and how to prevent mistakes when it comes to clarifying "ownership" rights of data takes good *architecture*. This is precisely the kind of framework proposed here in order to balance intuition and rationality. In other words, the ideas underlying the contractual model of this research is to make the laborious work of System 2 easily accessible for end-users and Cloud providers so they can make better and faster decisions. The overall idea is to have a systematic SLA framework in order to improve decision-making. This will reduce deliberation and transaction costs and will optimize Cloud computing transactions.

[100]Sunstein (2014), pp. 63–99; Corrales and Jurčys (2016), pp. 533–536.

[101]Sunstein (2014), pp. 66–99, 119–158; Sunstein (2013a).

[102]Corrales and Jurčys (2016), pp. 533–536.

This section explains how the simple idea of nudges in Cloud brokerage architectures can align with SLAs making them less complicated. SLAs are not drafted in a vacuum. They are made in an environment where many components and features converge. This being said, the correlation between nudges, choice architectures and SLAs are of equal importance when drafting an SLA, if not the most important thing for targeting various stakeholders at the global scale. Why should Cloud providers care? Many Cloud providers do not understand or simply resist the idea that clarifying legal issues is a key contributor to end-user's quality of service, which then contribute to building trust and potentially bringing more customers on board. In order to provide a more well-rounded view, this section offers a brief and non-exhaustive list of the key points to be remembered from our earlier discussions about nudges and choice architectures. All of the below should be generally taken into account as nudges[103] that can help at every level of Cloud computing transactions.

(i) An effort to raise awareness about the main legal issues that should be taken into account. In this case, the focus is on the addition of more capabilities and/or parameters required to achieve dynamic management of "ownership" rights of data;
(ii) An effort to provide concise, clear and simple information about legal rights;
(iii) An effort to inform the involved parties about the importance of clarifying "ownership" rights of data;
(iv) A disclosure mechanism imposed on Cloud providers that collates the information with end-user specification requirements so that end-users can clearly see whether the target infrastructure provider meets the eligibility criteria for a specific service requested;
(v) A default rule designed to clarify "ownership" rights of data;
(vi) Graphic warnings and reminders that alert the involved parties about the potential legal risks so they have the freedom to choose a different "route";
(vii) An initiative (e.g., through standardization) by which Cloud brokers can urge Cloud providers to disclose information that enables end-users to track and find the providers that best fit their needs. This information might be in machine-readable format or may be converted to such a form by the broker.

This list is just a sampling of the nudges that have to be implemented in the contractual framework. More will be said about this in the following sections when the specifications of SLAs are examined in more detail. The overall idea is that with some kind of soft nudging techniques implemented already in the architecture design, SLAs can radically improve. As hinted earlier, it turns out that the solution is not in clarifying the contractual clauses per se. That is only one part of the equation. What we also need to do is to change the architecture design of the SLAs by creating more choices and implementing effective nudging techniques, not only

[103]In this section, the basis for nudges in SLAs are inferred to be similar in certain aspects to other kind of nudges explained by Cass Sunstein. See Sunstein (2013b), pp. 38–39; see also generally Minton and Kahle (2013); Thaler et al. (2010).

between end-users and Cloud providers but also essentially between Cloud brokers and Cloud providers. Cloud brokers can create the interface to enable improved choices between end-users and Cloud providers.

One of the central ideas of this research is to make SLAs more useful and universally accessible. Therefore, the information presented in the SLA is very important. While making hasty decisions, end-users may be sometimes influenced by their own biases, ignoring the probabilities and underestimating the risks involved. "We are often confident even when we are wrong, and an objective observer is more likely to detect our errors than we are" as Kahneman ably put it.[104] This is the reason why it is suggested that brokerage services can best play the role of that subtle "objective observer." Therefore, the broker who is responsible for creating the programing code and the descriptions of the SLA based on an XML[105] automated framework is one of the main "choice architects." Cloud brokers can give end-users and Cloud providers some helpful warning nudges through the XML Description Schema that is presented in the following sections. Therefore, "ownership" rights of data can only be successfully achieved if incorporated at early stages of the design architecture and taken into account through the whole lifecycle of the Cloud service provision. This includes the technical implementation of warning signals to improve decision-making without coercion. As an example, various ranking mechanisms exist for translating SLA terms to more meaningful and abstracted (to the end-user) metrics such as SLA strictness. Whether or not a specific term is of interest to a specific end-user could be formulated as choice questions, driving the broker to include or not that term's effect in the final ranking.[106]

To explain this in simple terms, this framework will essentially operate as in the GPS example above. It will signal in a way the best "route" to take by sending some warning signs with regard to specific legal issues. This will allow the involved parties more freedom to continue or change their course of action. This is the kind of paternalism that does not override people's freedom and judgments about their own ends. The same question about the legitimacy of the government to softly nudge its citizens as a kind of "libertarian paternalism" or "soft paternalism" in Sunstein's narrative could be posed to Cloud brokers. The main question would be whether Cloud brokers could act paternalistic? Or, to put this in other words, to what extent can Cloud brokers step in when there are cases of market failures? Especially where people are likely to err and it is necessary to provide the means for improved decision-making. In our view, the "paternalistic" intervention of Cloud brokers could be legitimized in some instances if we take the *soft* paternalistic approach in Sunstein's narrative as in the GPS iconic example. Below, the type of nudging technique that will be specifically embedded in the architecture design of the computer code is explained.

[104]Kahneman (2011), p. 4.

[105]XML is a markup language standard that aims to define a format that is both human and machine understandable.

[106]See generally, Herbst et al. (2016).

6 Default Rules and Information Disclosure as Prime Nudges

A key nudging strategy refers to default rules and information disclosure. According to Sunstein, freedom of choice is emphatically a good thing and it is always present in our daily life and business, as well as in our social and political participation. Some may argue that in a democratic society this is a blessing.[107] Yet, it may also become a burden when too many choices present themselves and we do not know what to choose.[108] Choosing takes time and effort. It requires a great deal of study and deliberation. Thus, choosing may become a source of anxiety. Sometimes, "choosing not to choose" is a better option that can yield lower transaction and deliberation costs, making it more cost-effective for end-users. This can also improve their social welfare and respect their freedom.[109] That choice is of particular interest in Cloud computing contracts, since it leaves considerable room for end-users to focus on what it matters for their own businesses.

On this account, default rules are probably one of the most efficient possible nudges. Disclosure requirements fall into the same category too. They can have a significant and lasting impact since they tend to stick.[110] They are "ubiquitous" and very powerful.[111] The GPS system can serve here again as an example of a prime nudge. The GPS system is an electronic device set out as a default mechanism. It enables individuals to choose not to choose the best route available to their destination. It selects a "default route" allowing them to exercise their freedom by following or ignoring the route. In this era of technology,[112] with the coming of Cloud-based computing and fully automated contracts, it is now possible to identify tailor-made default rules to end-users' needs. Contracts can consist, in large measure, of default rules. Thus, applying a series of default rules as prime nudges can aid to personalize and enhance the efficiency of SLAs. The contractual framework that we will present in the next section will include an XML schema with a set of pre-defined parameters necessary for choosing a Cloud provider accordingly. More specifically, the XML-based definition schema contains customized default rules that can help to clarify "ownership" rights of data and databases in an automated fashion.

There are many reasons that can justify this approach. Consider the following legal comparisons. People are often allowed to negotiate their rights. In many legal

[107]Sunstein (2015), Preface.

[108]See, e.g., Iyengar and Lepper (2000), pp. 995–1006. In this empirical research, the authors challenged the assumption that the more choice, the better. In 3 different experiments, they arrived at the conclusion that people are more likely to choose or buy something when limited choices are available. For example, it is easier to choose and buy jam or chocolate from a limited array of 6 options rather than a more extensive selection of 24 or 30 choices.

[109]Sunstein (2015), p. 173.

[110]Sunstein (2013c), p. 11.

[111]Thaler et al. (2013), p. 430.

[112]Sunstein (2015), Preface, p. 6.

systems people can exercise their rights by default but they can also forsake specific rights. In most civil cases and even some criminal actions, individuals can waive their rights to sue before court. They can also exchange their ownership titles in return for something. The same rules shall apply by analogy to "ownership" rights of data. The SLA will essentially embrace the choice to "trade" or "waive" such rights, which are typically not covered in Cloud transactions. These capabilities are now included by default in the OPTIMIS toolkit.[113] Another parallel can be drawn from financial agents and the general power of attorney for administrative or legal acts. People hire trustworthy agents based on their skills and expertise. They authorize them to act on their behalf for a wide-range of financial, economic and legal aid. Under these circumstances, people act as "principals," hiring agents to replace them when needed. In other words, they are choosing not to choose. In the same vein, the main thesis of this research puts forward a number of tools and practical solutions through the agency of a broker as a representative of end-users. For present purposes, therefore, the crucial point is to recognize, by analogy, that end-users are relying on the broker's ability to elicit and convey information from Cloud providers based on the automatic default settings incorporated into the SLAs. In doing so, they are also choosing not to choose.[114]

7 A Sui Generis Contractual Framework

This Sui Generis Contractual Model is based on a SLA and a service manifest, which establishes the relationship between the involved parties. The SLA and service manifest consist of different parts including a specific legal section. The SLA template basically contains some mandatory legal tags. Furthermore, it also allows the possibility to attach framework contracts concluded by the parties. Framework contracts are additional agreements between the parties that may not be technically feasible to implement in the SLA and service manifest.[115] Yet, they could be added to the contractual framework by making reference to them in the SLA. This distinction is very important for it allows flexibility to the contractual framework in case any remaining legal issue needs to be additionally clarified. Nevertheless, a very important function of this unique framework is to emphasize that making decisions about "ownership" rights of data and databases should also be incorporated at the earlier stages of the architectural design.

---

[113]OPTIMIS is an open source toolkit designed to help Cloud service providers to build and run applications in the Cloud. New features that include the clarification of database rights and "ownership" rights of data have been implemented. The toolkit has been integrated into the OpenNebula Ecosystem and the Infrastructure-as-a-Service Cloud computing project OpenStack. See EU Project Enhances Open Source Toolkit Cloud; see also XML Description Schema Improvement.

[114]Sunstein (2015), pp. 8–9.

[115]Cloud Legal Guidelines (Final Report), Deliverable 7.2.1.4, p. 14.

As seen above, the arrival of Cloud computing poses great challenges concerning the manipulation of data and databases, specially in hybrid Clouds where end-users lack the knowledge and expertise to deal with all the complexities of Cloud transactions. The aim of this section is to explain in more detail the contractual framework that includes the clarification of "ownership" rights of data and databases. This is necessary for selecting the correct Cloud provider for the outsourcing and sharing of data and databases in an automated fashion. Thus, the clarification of these rights may be seen as a legal constraint embedded in the software architecture as proposed by Lessig in the New Chicago School approach.[116] In addition, this can also be framed as improved choices as indicated by Thaler and Sunstein in the Behavioral Law and Economics narrative. This Sui Generis Contractual Model can be checked in a machine-readable way in order to fully grasp the potential of Cloud computing and Big Data. Therefore, a mechanism where customers are under more control when using Cloud and Big Data services is proposed. Such a mechanism aims to provide them with the possibility of keeping their rights or waive them depending on their location and specific needs by selecting the infrastructure provider using a specific XML schema during the SLA negotiations.

The information provided in this framework should be used in order to automate the negotiation process between the broker and the Cloud infrastructure providers in Cloud brokerage scenarios. The main purpose of providing such an XML-based definition is to provide a "*template*" to bridge the gap between end-users and Cloud providers in order to grant end-users the capacity to choose a Cloud provider accordingly. The XML may be edited by humans based on a template model, and the produced created instance can be processed by according software, following a relevant decision logic. For example, the template model dictates the available fields, the user selects the according values, and then the relevant software may retrieve the XML-based provider descriptions and filter them based on the user's requirements.[117]

This section takes into account the previous work related to the OPTIMIS European funded project concerning the XML definition for data protection and security issues[118] and extends the work to include "ownership" rights of data. In the past, XML-based descriptions have been taken into account mainly for the SLA definitions, but not in the pre-selection of infrastructure providers to match the client needs. They usually refer only to how many resources one would get. Some SLAs have been extended with some textual input, but mainly from a contractual point of view (which is not machine understandable and thus it is a kind of "take it or leave it" form of contract). Therefore, with this new approach, it is possible to

[116]See, e.g., Lessig (2006).

[117]See, e.g., Kousiouris et al. (2013), pp. 63 et seq.

[118]Barnitzke et al. (2011), pp. 51–55.

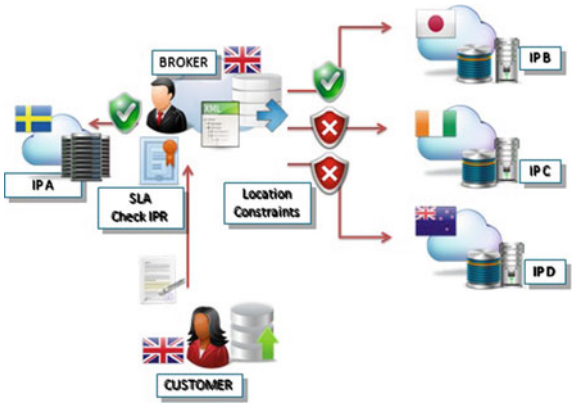

Fig. 1 Cloud broker service for the clarification of "ownership" rights

pre-filter Cloud providers that do not meet the legal requirements based on end-users input.

Currently, there is no such automated procedure for checking whether "ownership" rights of data are clearly defined and specified so that a broker can "on the fly" and automatically confirm the legal compliance. These options may be inserted as legal requirements from the user side and be used by the Cloud broker during the selection process.[119] As seen earlier, the broker is an entity positioned between customers and Cloud providers who need to find out which provider suits the demands requested in the SLA. Depending on the active role the broker is going to take during the brokerage process as a third party, it can act as a mere intermediate or can also take an active part during SLA negotiations and selection of the Cloud providers. The complete process is graphically explained below in Fig. 1. In this hypothetical scenario, the main responsible actor is the broker located in the UK. The broker receives the legal requirements from the customer and must act accordingly. In any case, the broker must choose from a constellation of infrastructure providers (IP A, IP B, IP C and IP D). This will depend on the legal requirements selected by the Cloud customer as a location constraint mechanism.

8 Automated Framework: The "Dead Man's Switch"

In order to attain the full potential offered by dynamic Cloud transformations, a suitable declaration procedure that meets these legal requirements must be implemented. This will provide more flexibility and scalability, while relaxing some of the cumbersome bureaucratic procedures such as the manual checking of contractual clauses. This section explains in detail the main features of the legal framework

[119]Kousiouris et al. (2013), p. 63.

that must be embedded through a suitable XML schema. Within this framework, infrastructure providers should take the XML schema and fill in with their own information, and then make it available to the public.[120] Therefore, Cloud brokers can read this information during the selection of infrastructure providers procedures as follows: First of all, the infrastructure providers must enforce a mechanism that declares the locations of their data centers as this will establish the jurisdiction and, therefore, the applicable law. The information related to the location of data centers is possibly one of the most important factors. This information must be included and displayed by an infrastructure provider that needs to be suitably adapted to a machine-readable way so it can be processed in an automated fashion. This information is usually exposed for the purposes of the infrastructure provider selection procedure in different group categories. Frequently, there is a legal information category that focuses on data protection and security issues.[121] Therefore, this section aims at extending these capabilities so as to include "ownership" rights of data and databases.

The benefits of this automated and embedded system approach can be best explained by referring to the so-called "dead man's switch." The general principle behind the "dead man's switch"—also known as a "kill switch" or "dead man control"—is to reduce the chances of making mistakes and having accidents. The Academic Press Dictionary of Science and Technology defines this term as follows: "a safety mechanism requiring constant pressure or manipulation by human operator; it stops a machine or vehicle automatically if the operator becomes incapacitated or inattentive."[122] They are frequently used in the operation of heavy machinery and electronic devices such as: trains, roller coasters, ships, tread machines, tractors, lawn mowers, freight elevators and many medical devices. The "kill switch" works automatically in cases where the person becomes unable to drive or operate the machine such as through death, falling asleep, loss of consciousness, illness, poisoning, etc.[123]

This concept was originally applied to subway and railroad systems.[124] A tragic story occurred on 27 April 2010, when a driver operating a train in the US apparently suffered a severe heart attack. When this happened, the "dead man's switch" kicked in. The train stopped immediately when the driver took his hand off

[120]The XML schema was made in the Eclipse Integrated Development Environment (IDE), which is a graphical tool for creating code (and other things such as the xml example). By having the schema model file, an interested entity may import it in a programming environment such as the Eclipse IDE. Based on the schema (also known as "xsd file" in reference to the file name extension ".xsd"), they can create an instance and populate the individual values (or select from value lists where this input is limited to a predefined selection). More details on this process can be found in Vafiadis et al. (2012), pp. 27–31.

[121]See, e.g., Kousiouris et al. (2013), pp. 63 et seq.

[122]Morris (1992), p. 591.

[123]See Guastello (2014), p. 253; Brauer (2016), p. 172; Anthony (1995), p. 93.

[124]See, e.g., Cunningham and Hart (1993), p. 24.

the control system.[125] This concept was then transferred to apply to other vehicles and machinery. For example, lawn mower machines now need to be activated by pressing a secondary bar together with the main handle. If the person operating the machine releases the secondary handle, the mower blade stops spinning automatically. This mechanism may prevent potential accidents if the person cutting the grass stumbles or becomes otherwise incapacitated.[126] Treadmills at the gym are also good examples of "dead man's switch." They often have a safety magnetic cord that the runner clips to her waist. If the runner moves too far away or is falling, the safety magnet will pull out away from the treadmill and the machine will stop immediately.[127] The dead man's feature is now applied to describe other intangible software features. Perhaps a better term to characterize this in the software domain would be "enabling devices," as the term "dead-man switch" might send the wrong message.[128] Nevertheless, for the sake of analogy and for the purpose of understanding the software features and SLA specifications, the "dead man's switch" can serve as a good example for the XML description explained in detail below.

9 XML-Based Description Schema

The SLA and service manifest itself contains an XML-based Description Schema. Figure 2 below shows the graphical representation of this schema. The figure includes a number of fields that are dictated by the relevant legal analysis and intellectual property compliance capabilities and is readily available and offered in the OPTIMIS platform via an Hypertext Transfer Protocol (HTTP) GET[129] interface (getCPdescription).[130] The left column of Fig. 2 shows the high level categories of legal aspects (e.g., ability to define location of the service, Standard Contractual Clauses (SCC), Intellectual Property Compliance, Data Portability, etc.). For example, SCC Compliance Types correspond to the legal analysis with regard to the EU Data Protection Framework. For each of these categories, new specialization types are defined in the right column, indicating specific fields or necessary information for each case.

What is of specific interest in the discussion of the present study is the "Intellectual Properties Compliance Type" section as depicted in more detail below in Fig. 3. The "Intellectual Properties Compliance Type" section has been specifically implemented and expanded to address the research questions of this chapter. Some sections include

[125]Newman (2010).

[126]Ostroff (2011), pp. 10–12.

[127]Bayles (2014), p. 331.

[128]Nix (2011).

[129]An HTTP Get operation is a simple type of web service from which one can retrieve formatted information, similar to a request in a standard browser for a web page.

[130]Kousiouris et al. (2013), pp. 64–65.

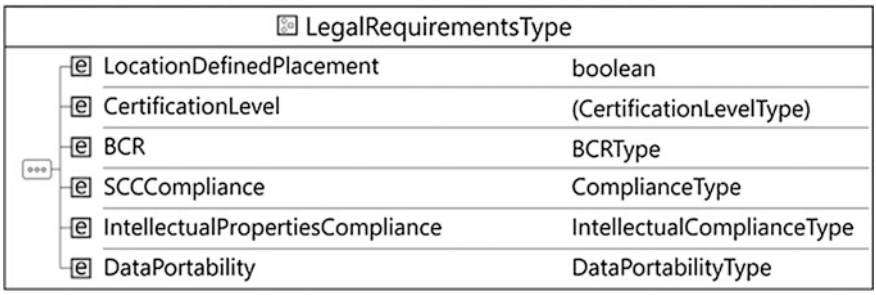

Fig. 2 Legal requirements—high level perspective

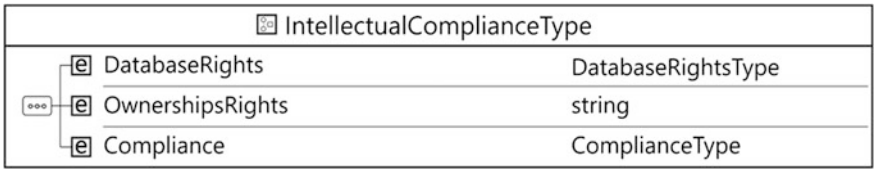

Fig. 3 Intellectual property compliance type

"string" (textual) variables that allow, programmatically, the possibility to include legal text in plain English language. Other sections are set out as "Boolean" data types. Booleans are data types that contain two values typically denoted as true or false. This section has been broken down in three main parts: (a) database rights, (b) "ownership" rights, and (c) compliance, as shown in Fig. 3. The database rights section (DatabaseRightsType) is again divided into three parts as indicated in Fig. 4. This section includes the following: (1) a location constraint mechanism (LocationType), which allows the Cloud provider to choose in which countries the databases are going to be located; (2) a "Boolean" waiving system (WaiveRights Boolean), whereby the Cloud provider can choose to keep or waive database rights; (3) a "string" field capability (Clause string), which allows the inclusion of contractual clauses written in plain English as defined by the provider on a case by case basis. Finally, the "Compliance Type" section contains a "string" field variable, which may also be validated by a respective Certification Authority. Moreover, this section also contains a "Compliance Flag" mechanism that will be activated immediately based on the geographic location restrictions according to end-user's criteria.

The complete process is as follows:

(i) The Cloud broker issues the XML template with the new available choices;
(ii) The Cloud providers use the template to create their description;
(iii) The user dictates which of the options they need activated. In order to do so, user input may be obtained from web forms that are automatically created

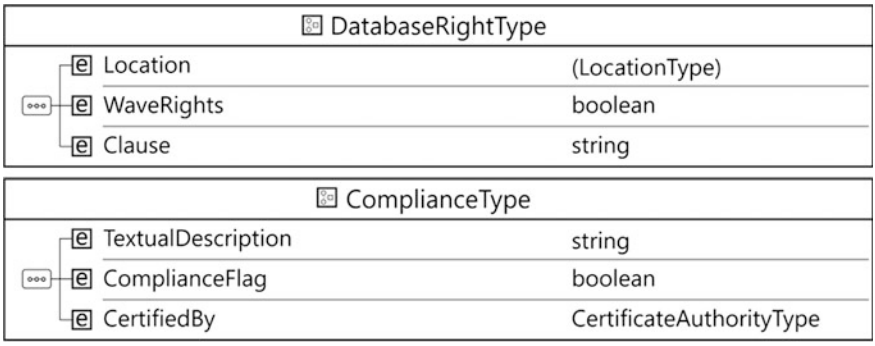

Fig. 4 Database right and compliance type section

from schema/template files through e.g., tools like XML Schema Definition (XSDForm)[131];

(iv) The Cloud broker compares the user requirements against the provider description.

The Cloud broker performs this definition when they define the Cloud Provider Description Template (CPDT), in order to limit provider input. This way the software behind the logical processing may directly compare user-selected input with the necessary textual concept. The OPTIMIS toolkit can be downloaded from the OPTIMIS website (http://optimistoolkit.com). It has been now updated and expanded with an automated XML Description Model for clarifying "ownership" rights of data and databases. More specifically, the description can be accessed from the following website: (http://www.optimis-project.eu/content/xml-description-schema-improvement) and used by the broker or by any of the parties depicted in the Cloud brokerage scenario.

Thereafter, the content of the XML description may be checked directly by using the Data Manager in the OPTIMIS platform. This method collates the information published by the infrastructure provider with the user specification requirements (e.g., location of provider, intellectual properties) and finally concludes the agreement if the target infrastructure provider meets the eligibility criteria for a specific service requested.[132] To explain how this technical process works in simple words, we can refer to the "dead man's switch" analogy. The proposed SLA framework is based on a technology that enables the enforcement of specific legal requirements. This can be achieved by using a tag list of certain legal criteria that is automatically activated. Thus, the federation of data and databases does not take place if the target providers do not run their services based on end-users' requirements. To be more specific, if we take any of the "dead man's switch" examples, the federation will not

[131]See, e.g., Ilerian, XSD Form Features Overview.

[132]Kousiouris et al. (2013), p. 68.

proceed if one of the processors or sub-processors does not run their data centers within the specifications of the given SLA framework.

10 Conclusion

In this chapter, we have analyzed the so-called "bounded rationality" principle, by which all human beings have flaws and limitations. As such, they have a tendency to take impulsive decisions. They are also unrealistically optimistic and are strongly affected by default rules. Because they are prone to procrastination and often think in a short-term perspective, default rules can create a lot of damage (but also can create a lot of good). The advantages of this cognitive-biased approach are evident. System 1 is a doer, not a planner, whereas System 2 thinks more about the probabilities. Understanding how people think and how they fail to plan can help us to design better choice architecture environments.[133] By extension, such insight can also be put in making default mechanisms to better shape SLAs in the Cloud.

This is where the notion of trust comes to the fore as a venue to justify the role of choice architects in nudging people. The motivation for this is that there are not sufficient thoughts about the relationship between behavioral law and economics and SLAs in the Cloud. Therefore, this is an effort to engage in such a debate. To fit the legal questions of this research, Cloud architectures and in particular SLAs have to be thoroughly redefined in relation to "ownership" rights. The suggestion here is to reform Cloud architectures and selections founded in the belief and abilities of nudges. This argument was developed on a small scale and regarding the specific problem of clarifying "ownership" rights of data that can make a big difference as a whole.

As for the question of choice architecture, the reasoning behind some of the nudge ideas is persuasive. The default settings in the printer machine and GPS examples remind us of what Lessig said in his book *Code Version 2.0*. He extended the notion of regulation to include not only legal structures but also technological architectures written in software and hardware codes. This was also a reaction to libertarianism due to the outpouring of liberal ideas with the advent of the Internet.[134] Similar to the typical and old software engineering truisms, choice architectures capture broadly-applicable principles of software and hardware construction, where designing more customized applications and options as default rules can lead users to make better decisions.

The advantages of thinking about the improvement of choice architectures are manifold. This notion encompasses various dimensions of "frame choices" on the normative level. It is contingent on Cloud architectures where brokers are allowed to use various active nudging techniques to influence Cloud providers and as a corollary improve the decision-making of end-users. This new flow of "indirect

[133]Sunstein (2015), pp. 12–13.

[134]Lessig (2006), pp. 1–432.

nudging" techniques itself breeds a new paradigm. Improved choices, warning signals, information disclosures and default rules should be embedded in the architecture and operations design of software. This will reduce deliberation costs, improve welfare and enhance the efficiency of Cloud computing transactions. It will also increase the likelihood that the involved parties will be better off. The bottom line is: since architectures are inevitable and since choice architects will bias decisions in one way or another, ignoring them is not an option. On the contrary, this will make choice architectures more likely to be poor or in favor of choice architects. The operative broader question is not to nudge end-users but to approach Cloud providers so they can improve choice architectures and influence better decision-making.

Acknowledgements In developing the concepts described in this chapter, we had the opportunity to learn from many people. We would like to thank Prof. Toshiyuki Kono, Prof. Shinto Teramoto, Prof. Mark Fenwick, Paulius Jurčys and Rodrigo Afara. This chapter was partially funded by the Monbukagakusho-MEXT Japanese government scholarship program and the Optimized Infrastructure Framework (OPTIMIS) EU funded project within the 7th Framework Program under contract ICT-257115.

References

Abbots E, Lavis A (eds) (2016) Why we eat, how we eat: contemporary encounters between foods and bodies. Routledge, London

Abraham R, Aier S, Winter R (2012) Two speeds of EAM-A dynamic capabilities perspective. In: Aier S et al (eds) Trends in enterprise architecture research and practice-driven research on enterprise transformation, 7th workshop, TEAR 2012, and 5th working conference, PRET 2012, Proceedings. Springer, Berlin

Adhikari A, Adhikari J (2015) Advanced in knowledge discovery in databases, vol 79. Springer, Cham

Al-khouri A (2012) Data ownership: who owns 'My Data'? Int J Manag Inf Technol 2(2):1–8

Anger E (2016) A course in behavioral economics, 2nd edn. MacMillan Education Palgrave, London

Anthony S (1995) Farm and ranch safety management (agriculture). Delmar, Cengage Learning, Clifton Park

Angner E, Loewenstein G (2016) Behavioral economics, Elsevier's handbook of the philosophy of science, vol 5. http://www.cmu.edu/dietrich/sds/docs/loewenstein/BehavioralEconomics.pdf. Accessed 10 Jan 2017

Avineri E (2014) Nudging safer road behaviors. http://www.rannaorf.org.il/webfiles/files/Nudge_in_Road_Safety_final.pdf. Accessed 1 Sept 2016

Balasubramanyam S (2013) Cloud-based development using classic life cycle model. In: Mahmood Z, Saeed S (eds) Software engineering frameworks for the cloud computing paradigm. Springer, London

Barnitzke B et al (2011) Legal restraints and security requirements on personal data and their technical implementation in clouds, Workshop for E-contracting for clouds. eChallenges. http://users.ntua.gr/gkousiou/publications/eChallenges2011.pdf. Accessed 1 Sept 2016

Bayles M (2014) Exercise testing. In: Swain D (ed) ACSM's resource manual for guidelines for exercise testing and prescription, 7th edn. Wolters Kluwer (Lippincott Williams & Wilki), Philadelphia

Behavioral Insights Team. http://www.behaviouralinsights.co.uk. Accessed 1 Sept 2016
Béranger J (2016) Big data and ethics: the medical datasphere. ISTE Press Ltd., London
Berman J (2013) Principles of big data: preparing, sharing, and analyzing complex information. Morgan Kaufmann (Elsevier), Waltham
Biddle S, Mutrie N, Gorely T (2015) Psychology of physical activity: determinants, well-being and interventions, 3rd edn. Routledge, London
Bishop M (2009) Essential economics: an A to Z guide. The economist, 2nd edn. Bloomberg Press, New York
Biswas S (2014) Relationship marketing: concepts, theories and cases, 2nd edn. PHI Learning Private Limited, Delhi
Bloomberg J (2013) The agile architecture revolution: how cloud computing, rest-based SOA, and mobile computing are changing enterprise IT. Wiley, Hoboken
Blythe J (2013) Consumer behavior, 2nd edn. Sage, Los Angeles
Brauer R (2016) Safety and health for engineers, 3rd edn. Wiley, Hoboken
Brown D (1972) Mill on liberty and morality. Philos Rev 87(2):133–158
Businessballs.com. Nudge theory. http://www.businessballs.com/nudge-theory.htm. Accessed 1 Sept 2016
Bygrave L, Bing J (eds) (2009) Internet governance: infrastructure and institutions. Oxford University Press, Oxford
Catlett C (2013) Cloud computing and big data. IOS Press, Amsterdam
Chen M et al (2014) Big data: related technologies, challenges and future prospects. Springer, Cham
Clark G, Strauss K, Knox-Hayes J (2012) Saving for retirement: intention, context, and behavior. Oxford University Press, Oxford
Clark R (2010) I'm just saying. Dog Ear Publishing, Indianapolis
Clements P et al (2010) Documenting software architectures: views and beyond, Carnegie Mellon Software Engineering Institute (SEI) series in software engineering, 2nd edn. Addison Wesley, Upper Saddle River
Cloud Legal Guidelines (final report), Deliverable 7.2.1.4. http://www.optimis-project.eu/sites/default/files/content-files/document/optimis-public-deliverable-d7214-Cloud-legal-guidelines-final-report.pdf. Accessed 1 Sept 2016
Corrales M et al (2010) Intellectual property rights in e-health: balancing out the interests at stake—a Herculean task? Int J Priv Law 3(3):286–299
Corrales M, Jurčys P (2016) Review of Cass Sunstein, why nudge: the politics of libertarian paternalism. Yale University Press, New Haven/London (2014). Mod Law Rev 79:533–536
Corrales M, Jurčys P (2016) A new legal landscape for big data in Japan. Beck-Online, ZD-Aktuell 15 (05247)
Connolly D, Coburn P (2016) Legal theory and the relationship between psychology and law. In: Jackson R, Roesch R (eds) Learning forensic assessment: research and practice, 2nd edn. Routledge, New York
Consumer Policy Toolkit, Organisation for Economic Co-operation and Development. http://www.oecd.org/sti/consumer/consumer-policy-toolkit-9789264079663-en.htm. Accessed 1 Sept 2016
Crawford L (2015) JAPAN: new amendments to Japanese privacy law. http://blogs.dlapiper.com/privacymatters/new-amendments-to-japanese-privacy-law/. Accessed 1 Sept 2016
Cunningham J, De Hart L (1993) A history of the New York City subway system, revised edition, s. l
Dold M (2016) Condorcet's jury theorem as a rational justification of soft paternalistic consumer policies. In: Mathis M, Tor A (eds) Nudging—possibilities, limitations and applications in European law and economics. Springer, Cham

Elkin-koren N, Salzberger E (2013) The law and economics of intellectual property in the digital age: the limits of analysis. Routledge, London
English Collins Dictionary. http://www.collinsdictionary.com/dictionary/english/nudge. Accessed 1 Sept 2016
Eppinger S, Browning T (2012) Design structure matrix methods and applications. The MIT Press, Cambridge
EU Project Enhances Open Source Toolkit Cloud. http://www.optimis-project.eu/sites/default/files/content-files/document/eu-project-enhances-open-source-toolkit-Cloud-2.pdf. Accessed 1 Sept 2016
Evans J (2003) In two minds: dual-process accounts of reasoning. Trends Cogn Sci 7(10):454–459
Evans-Pritchard B (2013) Aiming to reduce cleaning costs, works that work. https://worksthatwork.com/1/urinal-fly. Accessed 1 Sept 2016
Executive Order (2015) Using behavioral science insights to better serve the American people, The White House, office of the press secretary. https://www.whitehouse.gov/the-press-office/2015/09/15/executive-order-using-behavioral-science-insights-better-serve-american. Accessed 1 Sept 2016
Felin T (2014) Nudge: managers as a choice architect, the Saïd Business School's working paper series, University of Oxford. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2523922. Accessed 1 Sept 2016
Gigerenzer G (2000) Adaptive thinking: rationality in the real world. Oxford University Press, Oxford
Gigerenzer G, Selten R (eds) (2002) Bounded rationality: the adaptive toolbox. The MIT Press, Cambridge
Gigerenzer G (2015) On the supposed evidence for libertarian paternalism. Rev Philos Psychol 6 (3):361–383
Guastello S (2014) Human factors engineering and ergonomics: a systems approach, 2nd edn. CRC Press, Boca Ratón
Hamilton D, Zufiaurre B (2014) Blackboards and bootstraps: revisioning education and schooling. Sense Publishers, Rotterdam
Hartley D (2012) Education and the culture of consumption: personalisation and the social order. Routledge, London
Herbst N et al (2016) Ready for rain? A view from SPEC research on the future of cloud metrics, SPEC RG cloud working group. Technical report, version 1.0. https://arxiv.org/pdf/1604.03470.pdf. Accessed 5 Jan 2017
Heshmat S (2011) Eating behavior and obesity: behavioral economics strategies for health professionals. Springer, New York
Heukelom F (2014) Behavioral economics: a history. Cambridge University Press, New York
Horten M (2016) Closing of the net. Polity Press, Cambridge
Ilerian. XSD form features overview. https://ilerian.com/overview. Accessed 1 Sept 2016
Iyengar S, Lepper M (2000) when choice is demotivating: can one desire too much of a good thing? J Pers Soc Psychol 79(6):995–1006
Jackson J (2006) Ethics in medicine: virtue, vice and medicine. Polity Press, Cambridge
Jamson S (2013) The role of acceptance in behavioral adaptation. In: Rudin-Brown C, Jamson S (eds) Behavioral adaptation and road safety: theory, evidence and action. CRC Press, Boca Ratón
Jansen A, Bosch J (2005) Software architecture as a set of architectural design decisions. In: Nord R et al (eds) 5th working IEEE/IFIP conference on software architecture WICSA 2005, papers and working session results, proceedings, Pittsburgh, Pennsylvania. IEEE Computer Society, Los Alamitos
John P (2013) Nudge, nudge, think, think: experimenting with ways to change civic behavior. Bloomsbury, London
Jolls C, Sunstein C, Thaler R (1998) A behavioral approach to law and economics. Stanf Law Rev 50:1471–1550

Kahneman D (2003) A perspective on judgment and choice: mapping bounded rationality. Am Psychol 58(9):697–720
Kahneman D (2011) Thinking, fast and slow. Penguin Books, London
Kannan R et al (eds) (2016) Managing and processing big data in cloud computing. Information Science Reference (IGI Global), Hershey
Kasemsap K (2015) The role of cloud computing adoption in global business. In: Chang V, Walters R, Wills G (eds) Delivery and adoption of cloud computing services in contemporary organizations. Information Science Reference (IGI Global), Hershey
Kousiouris G, Vafiadis G, Corrales M (2013) A cloud provider description schema for meeting legal requirements in cloud federation scenarios. In: Douligeris et al (eds) Collaborative, trusted and privacy-aware e/m-services, 12th IFIP WG 6.11 conference on e-business, e-services, and e-society, I3E 2013, Athens, Greece, Proceedings. Springer, Heidelberg
Lahti A (2010) Globalization & the Nordic success model—Part I. Ventus Publishing ApS, Frederiksberg
Le Grand J, New B (2015) Government paternalism: nanny state or helpful friend?. Princeton University Press, Princeton
Lessig L (1999) Code, and other laws of cyberspace. Basic Books, New York
Lessig L (2006) Code, version 2.0. Basic Books, New York
Lightman A (2002) Brave new unwired world: the digital big bang and the infinite internet. Wiley, New York
Maclean A (2009) Autonomy, informed consent and medical law: a relational challenge. Cambridge University Press, Cambridge
Mainichi Japan (2015) Revised personal information protection law enacted. http://mainichi.jp/english/articles/20150904/p2a/00m/0na/012000c. Accessed 1 Sept 2016
Marinescu D (2013) Cloud computing: theory and practice. Morgan Kaufmann, Waltham
Merriam-Webster dictionary. http://www.merriam-webster.com/dictionary/oxymoron. Accessed 1 Sept 2016
Metcalfe J (2013) Japan Railway Company apologizes for selling IC card data. The Wall Street Journal. http://blogs.wsj.com/japanrealtime/2013/07/29/japan-railway-company-apologizes-for-selling-ic-card-data/. Accessed 1 Sept 2016
Mill J (1859) On liberty. Oxford University Press, Oxford
Millham R (2012) Software asset re-use: migration of data-intensive legacy system to the cloud computing paradigm. In: Yang H, Liu X (eds) Software reuse in the emerging cloud computing era. Information Science Reference (IGI Global), Hershey
Minton E, Kahle L (2013) Belief systems, religion, and behavioral economics: marketing in multicultural environments. Business Expert Press, New York
Morris C (1992) The academic press dictionary of science and technology. Academic Press Inc. (Harcourt Brace Jovanovich Publishers), San Diego
Mosco V (2014) To the cloud: big data in a turbulent world. Routledge, New York
Mukherjee S, Loganathan S (2014) Role of broker in InterCloud environment. In: Mahmood Z (ed) Continued rise of the cloud: advances in trends in cloud computing. Springer, London
Muller H (2015) The big shift in IT leadership: how great CIOs leverage the power of technology for strategic business growth in the customer-centric economy. Wiley, Hoboken
Munro A (2009) Bounded rationality and public policy: a perspective from behavioral economics. The economics of non-market goods and resources, vol 12. Springer, Dordrecht
Murugesan S, Ananth A (2016) Cloud computing: an overview. In: Murugesan A, Bojanova I (eds) Encyclopedia of cloud computing. Wiley, Chichester
Newman A (2010) Not the first time the 'dead-man' switch did its job. http://cityroom.blogs.nytimes.com/2010/05/07/not-the-first-time-the-dead-man-switch-did-its-job/?_r=0. Accessed 1 Sept 2016

Nix D (2011) Why you should stop using the term 'deadman'. http://machinerysafety101.com/2011/03/28/why-you-should-stop-using-the-term-deadman/. Accessed 1 Sept 2016
Nudges.org (2008) Another visual trick to nudge drivers to slow down. http://nudges.org/?s=lake+shore+drive. Accessed 1 Sept 2016
Online Etymology Dictionary. http://www.etymonline.com/index.php?term=eureka. Accessed 1 Sept 2016
Ostroff E (2011) Universal design: an evolving paradigm. In: Preiser W (ed) Universal design handbook: building accessible and inclusive environments, 2nd edn. Advisory Committee on Accessibility (ACA) Access Design Subcommittee, McGraw-Hill, New York
Oxford Dictionary. http://www.oxforddictionaries.com/es/definicion/ingles_americano/nudge. Accessed 1 Sept 2016
Parsons M, Colegate P (2015) 2015: the turning point for data privacy regulation in Asia? http://www.hldataprotection.com/2015/02/articles/international-eu-privacy/2015-the-turning-point-for-data-privacy-regulation-in-asia/. Accessed 1 Sept 2016
Penguin Group (2011) Book review—Nudge: improving decisions about health, wealth, and happiness (by Richard H. Thaler and Cass R. Sunstein). Health Policy Newsletter 24(2). http://jdc.jefferson.edu/cgi/viewcontent.cgi?article=1733&context=hpn. Accessed 1 Sept 2016
Perry D, Wolf A (1992) Foundations for the study of software architecture. Softw Eng Notes 17 (4):40–52
Perry M (1988) Morality, Politics & Law. Oxford University Press, New York
Personal Information Protection Commission (2016). http://www.ppc.go.jp/en/. Accessed 1 Sept 2016
Pomerol JC (2012) Decision-making and action. Wiley, London
Prinz A (2013) Should the state care for the happiness of its citizens? In: Brockmann H, Delhey J (eds) Human happiness and the pursuit of maximization: is more always better?. Springer, Dordrecht
Quigley M, Stokes E (2015) Nudging and evidence-based policy in Europe: problems of normative legitimacy and effectiveness. In: Alemanno A, Sibony AL (eds) Nudge and the law: a European perspective, modern studies in European law. Hart Publishing, Oxford
Raisinghani M et al (2015) Cloud computing in the 21st century: a managerial perspective for policies and practices. In: Aljawarneh S (ed) Advanced research on cloud computing design and applications. Information Science Reference (IGI Global), Hershey
Ramanathan J, Rammath R, Desai A (2009) Adaptive IT architectures as a catalyst for network capability in government. In: Saha Pallab (ed) Advances in government enterprise architecture. Information Science Reference (IGI Global), Hershey
Reb J et al (2014) Performance appraisals as Heuristics judgments under uncertainty. In: Highhouse S, Dalal R, Salas E (eds) Judgment and decision making at work. The organizational frontiers series. Routledge, New York
Reidenberg J (1998) Lex informatica: the formulation of information policy rules through technology. Tex Law Rev 76(3):553–593
Riley J (2015) The right to liberty. In: Schefczyk M, Schramme T (eds) John Stuart Mill: über die Freiheit. Walter de Gruyter GmbH, Berlin
Rinaldi G, Stella D (2016) Slalom: legal and open model terms for cloud SLAs and contracts, final version D 2.2. http://slalom-project.eu/sites/slalom/files/content-files/article/SLALOM%20D2%202%20%2814Apr2016%29_v1.2.pdf. Accessed 5 Jan 2017
Robson P, McCowan A (1998) Property law (Green's Concise Scots Law), 2nd edn. Sweet & Maxwell, Edinburgh
Simon H (1955) A behavioral model of choice. Q J Econ 69(1):99–118
Simon H (1972) Theories of bounded rationality. In: McGuire C, Radner R (eds) Decision and organization (study in mathematics & managerial economics), 1st edn. North-Holland, Amsterdam
Simon H (1984) Models of bounded rationality: economic analysis and public policy, vol 1. The MIT Press, Cambridge

Simon H (1998) Rationality in Psychology and Economics. In: Katz A (ed) Foundations of the economic approach to law, interdisciplinary readers in law. Oxford University Press, Oxford
Simon H (1990) Invariants of human behavior. Annu Rev Psychol 41:1–20
Sommer J (2009) When humans need a nudge toward rationality. The New York Times. http://www.nytimes.com/2009/02/08/business/08nudge.html?_r=0. Accessed 1 Sept 2016
Srinivasan S (2014) Cloud computing basics. Springer, New York
Stanovich K, West R (2000) Individual difference in reasoning: implications for debate? Behav Brain Sci 23(5):645–665
Stanovich K (2010) Rationality and the reflective mind, 1st edn. Oxford University Press, Oxford
Sunstein C (ed) (2000) Behavioral law & economics. Cambridge University Press, Cambridge
Sunstein C (2013a) Deciding by default. Univ Pa Law Rev 162(1):1–57
Sunstein C (2013b) Why paternalism is your friend. New Republic. http://www.newrepublic.com/article/112817/cass-sunstein-simpler-book-excerpt-why-paternalism-your-friend. Accessed 1 Sept 2016
Sunstein C (2013c) Simpler: the future of government. Simon & Schuster, New York
Sunstein C (2014) Why nudge? The politics of libertarian paternalism. Yale University Press, New Haven
Sunstein C (2015) Choose not to choose: understanding the value of choice. Oxford University Press, Oxford
Tanner M (2007) Leviathan on the right: how big-government conservatism brought down the republican revolution. Cato Institute, Washington
Thaler R, Sunstein C (2003) Libertarian paternalism is not an oxymoron, University of Chicago Public Law & Legal Theory, working paper no. 43. http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1184&context=public_law_and_legal_theory. Accessed 1 Sept 2016
Thaler R (2009) Opting in vs. opting out. The New York Times. http://www.nytimes.com/2009/09/27/business/economy/27view.html?_r=0. Accessed 1 Sept 2016
Thaler R, Sunstein C (2009) Nudge: improving decisions about health, wealth, and happiness. Penguin Group, New York
Thaler R, Sunstein C, Balz J (2010) Choice architectures. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1583509. Accessed 1 Sept 2016
Thaler R, Sunstein C, Balz (2013) Choice architecture. In: Shafir E (ed) The behavioral foundations of public policy. Princeton University Press, Princeton
The Economist (2006) The perils of prosperity: can you be too rich? http://www.economist.com/node/6849948. Accessed 1 Sept 2016
The Japan Times (2013) JR sells commuters' data. http://www.japantimes.co.jp/opinion/2013/08/03/editorials/jr-sells-commuters-data/#.V4L37Ev9opE. Accessed 1 Sept 2016
Utts J (2014) Seeing through statistics, 4th edn. Cengage Learning, Stamford
Vafiadis G, Kousiouris G, Nair S (2012) Data Manager (DM) user guide, OPTIMIS project. http://optimis-project.eu/sites/default/files/content-files/page/datamanageruserguide.pdf. Accessed 1 Sept 2016
Van Aaken A (2015) Judge the nudge: In Search of the legal limits of paternalistic nudging in the EU. In: Alemanno A, Sibony AL (eds) Nudge and the law: a European perspective. Hart Publishing, Oxford
Van Schewick B (2010) Internet architecture and innovation. The MIT Press, Cambridge
Veatch R (1997) Medical ethics, 2nd edn. Jones and Bartlett, Boston
Viale R (2012) Methodological cognitivism, vol 1: mind, rationality, and society. Springer, Berlin
Wallace D (2008) Plain old untrendy troubles and emotions. The Guardian. http://www.theguardian.com/books/2008/sep/20/fiction. Accessed 1 Sept 2016
White M (2013) The manipulation of choice: ethics and libertarian paternalism. Palgrave Macmillan, New York
White M (2016) The crucial importance of interests in libertarian paternalism. In: Mathis K, Tor A (eds) Nudging—possibilities, limitations and applications in European law and economics. Springer, Cham

Willis O (2015) Behavioral economics for better decisions, ABC.net. http://www.abc.net.au/radionational/programs/allinthemind/better-life-decisions-with-behavioural-economics/6798918. Thaler. Accessed 1 Sept 2016

Winston & Strown LLP (2015) Japan updates privacy law. http://www.winston.com/en/privacy-law-corner/japan-updates-privacy-law.html. Accessed 1 Sept 2016

Wright O (2014) The nudge team started out as a sort of mission impossible: how the government's successful behavior insights team has had a profound effect on Whitehall. Independent. http://www.independent.co.uk/news/people/profiles/the-nudge-team-started-outas-a-sort-of-mission-impossible-how-the-governments-successful-behaviour-insights-team-has-had-a-profound-effect-on-whitehall-9117793.html. Accessed 1 Sept 2016

World Development Bank Report (2015) Mind, science and behavior. http://www.worldbank.org/content/dam/Worldbank/Publications/WDR/WDR%202015/WDR-2015-Full-Report.pdf. Accessed 1 Sept 2016

XML Description Schema Improvement. http://www.optimis-project.eu/content/xml-description-schema-improvement. Accessed 1 Sept 2016

Zeiler K, Teitelbaum J (eds) (2015) Research handbook on behavioral law and economics. Edward Elgar Publishing, Northampton

A Brokering Framework for Assessing Legal Risks in Big Data and the Cloud

Marcelo Corrales and Karim Djemame

Abstract "Cloud computing" and "Big Data" are amongst the most hyped-up terms and buzzwords of the moment. After decades in which individuals and companies used to host their data and applications using their own IT infrastructure, the world has seen the stunning transformation of the Internet. Major shifts occurred when these infrastructures began to be outsourced to public Cloud providers to match commercial expectations. Storing, sharing and transferring data and databases over the Internet is convenient, yet legal risks cannot be eliminated. Legal risk is a fast-growing area of research and covers various aspects of law. Current studies and research on Cloud computing legal risk assessment have been, however, limited in scope and focused mainly on security and privacy aspects. There is little systematic research on the risks, threats and impact of the legal issues inherent to database rights and "ownership" rights of data. Database rights seem to be outdated and there is a significant gap in the scientific literature when it comes to the understanding of how to apply its provisions in the Big Data era. This means that we need a whole new framework for understanding, protecting and sharing data in the Cloud. The scheme we propose in this chapter is based on a risk assessment-brokering framework that works side by side with Service Level Agreements (SLAs). This proposed framework will provide better control for Cloud users and will go a long way to increase confidence and reinforce trust in Cloud computing transactions.

Keywords Cloud computing · Big Data · Service Level Agreements (SLAs) · Cloud brokers · Legal risks · Mutual trust

M. Corrales (✉)
Institute for Legal Informatics, Leibniz Universität Hannover, Hannover, Germany
e-mail: marcelo.corrales13@gmail.com

K. Djemame
School of Computing, University of Leeds, Leeds, UK

M. Corrales et al. (eds.), *New Technology, Big Data and the Law*,
Perspectives in Law, Business and Innovation, DOI 10.1007/978-981-10-5038-1_8

Contents

1 Introduction

Before embarking on the generally known caveats regarding legal risks, we would like to point out what Claudio Ciborra, an information theorist, has explained in his writings on information systems and risk management.[1] In what he called the "duality of risk,"[2] he reminds us "life, risk and technology are getting more intimate than ever…"[3] According to Ciborra, it is not just that our society is becoming increasingly dependent on mobile phones and computers as the primary means of communication; it is not about business transactions processed through electronic networks; it is not even about jobs being fully automated; or human reasoning being replaced by human-like artificial intelligence that emulates the decision-making of human experts.[4] Looking ahead and reflecting on the next generation of information communication technology (ICT) platforms and risk management, the challenge is that "our life (project) becomes simultaneously conditioned, constrained or enabled by Grid technologies. The technology is already there, albeit in an indirect and hidden form…"[5]

[1] Gutwirth and Hildebrandt (2010), p. 33.

[2] For details, see Ciborra (2005).

[3] Ciborra (2007), p. 27.

[4] For details about artificial intelligence (AI) and expert systems see, e.g., Jackson (1998).

[5] Ciborra (2007), p. 27.

Ciborra wrote the above lines more than ten years ago and Grid technologies evolved into different models.[6] As a matter of fact, Cloud computing is a kind of Grid computing, which focuses on the quality of service (QoS) and reliability problems.[7] The Cloud differs from the Grid essentially in the implementation details.[8] According to Ciborra, change and innovation brings the emergence of new risks, however, his vision goes beyond to suggest that risks are often the source of innovation[9] and new order.[10] As such, risk is not, in itself, a bad thing; rather, it is essential for accelerating progress.[11]

The aim of this chapter is to widen the lens through which we view risk and analyze particular kinds of legal risk connected to the design and deployment of Grid and Cloud computing infrastructures in brokerage scenarios.[12] This chapter presents an SLA brokering framework including innovative risk-aware assessment techniques, which facilitates the clarification of database and "ownership" rights of data and evaluates the probability of SLA failure. We use the web service agreement specification (WS-Agreement)[13] as a template and extend prior work on risk metrics from the OPTIMIS project[14] to facilitate SLA creation between service consumers and providers within typical Cloud brokerage scenarios. However, since the WS-Agreement allows for an automated mechanism between only two parties and does not cover the use of an intermediary within the agreement process, we use the specific work carried out in the AssessGrid project[15] that includes a brokerage mechanism and pays considerable attention to addressing a risk assessment.[16]

---

[6]For details about the evolution of Grid infrastructure technologies see, e.g., Jones and Bird (2013), pp. 160 et seq.

[7]Kasemsap and Sunandha (2015), p. 33.

[8]Teng and Magoules (2010), p. 126.

[9]Shantz (2005), p. 511.

[10]Ciborra (2009), p. 78.

[11]Drissi et al. (2013), p. 143.

[12]See, e.g., Gourlay et al. (2008), pp. 437–443.

[13]See Andrieux et al. (2007); see also Gourlay et al. (2008), p. 438. More specifically, for negotiating and creating SLAs, we use the WSAG4 J framework developed at Fraunhofer Institute SCAI. The WSAG4J is basically a tool that helps you to create and manage SLAs in distributed systems and has been fully implemented as part of the Open Grid Forum (OGF) WS-Agreement standard. For details, see https://packcs-e0.scai.fraunhofer.de/wsag4j/. Accessed 10 October 2016.

[14]Optimized Infrastructure Services (OPTIMIS) was a EU funded project within the 7th Framework Program under contract ICT-257115. The project developed an open source toolkit designed to help Cloud service providers to build and run applications in the Cloud. New features that include the clarification of database rights and "ownership" rights of data have been implemented. The toolkit has been integrated into the Open Nebula Ecosystem and the Infrastructure as a Service Cloud computing project Open Stack.

[15]The Advanced Risk Assessment and Management for Trustable Grids project (AssessGrid), was founded by the EU Commission under the FP6 IST framework (contract no. 031772).

[16]Padgett et al. (2009).

SLAs are facilitators for increasing the commercial uptake of Cloud computing services. They provide clear-cut rules concerning the expectations and obligations between service consumers and providers.[17] However, current frameworks fail to provide flexibility[18] and there is no global standard that clarifies database rights and more generally "ownership" rights of data. Therefore, it is always advisable to thoroughly check Cloud SLAs before being legally bound by the terms of contracts. Furthermore, without the ability to evaluate the probability that a SLA might fail, market growth will be limited, since neither party will be willing to agree. By introducing a database and "ownership" rights risk assessment alongside automated SLA creation and negotiation processes, end-users can uncover high-risk areas to attenuate such risks, and eliminate those Cloud providers that will not promote their needs.

This chapter is divided into 10 sections. Section 2 briefly reviews the extant literature with regard to risk assessment in the Cloud. It also explains the motivation and justification for deepening and expanding research into other areas of law such as database rights and "ownership" rights of data. Section 3 is concerned with the methodology used for this study, namely a risk-based approach through the whole service life cycle. Section 4 presents an overview of the legal risks involved and how a risk mitigation strategy will enhance legal interoperability. Section 5 delves into detail concerning database and "ownership" rights of data, focusing on the three key themes that create risk in Cloud computing and Big Data projects. Section 6 begins by offering a glimpse of the main actors involved. Then it goes on to explain the two general use cases considered. Finally, it explains the brokering mechanism and risk assessment techniques using WS-Agreement, which facilitates the creation of risk-aware SLAs between end-users and Cloud providers. Section 7 presents the risk inventory within the system architecture design. It includes an updated and customized risk inventory focused on the legal areas considered to present the higher risks and constrains. Section 8 explains step-by-step the different stages of the risk assessment process in Cloud brokerage scenarios. In Sect. 9 a hypothetical scenario is considered to showcase how risk assessment can be effectively applied in real cases. Finally, Sect. 10 concludes.

2 Risk Assessment: Literature Review, Motivation and Justification

As the realization of Cloud-based services and infrastructures advance[19] from one single private Cloud infrastructure, towards more complex migrations in dynamic federated scenarios consisting of several coexisting public or hybrid Clouds, there

[17]Djemame et al. (2011b), p. 1558.

[18]See, e.g., Kirkham et al. (2012), p. 1063.

[19]See Mahmood (ed) (2014).

are increasing high level concerns. These concerns include issues of risk, trust and legal considerations that establish solid foundations for the non-functional requirements[20] of the ecosystem. Cloud migrations have reached a high level of development, yet the management of Cloud services entails a loss of control over the data being processed. This also impairs the trustworthiness in Cloud computing technology because end-users are not entirely confident in using the Cloud.[21]

There are many legal risks involved that have been magnified by the Big Data movement to the Cloud.[22] The American Heritage dictionary defines risk as "the possibility of suffering harm or loss; danger." "A factor, thing, element, or course involving uncertain danger; a hazard."[23] Similarly, the Black's Law Dictionary defines risk as "the uncertainty of a result. Happening or loss; the chance of injury, damage or loss; esp., the existence and extent of the possibility of harm."[24] Therefore, the term risk can be loosely described as exposing oneself to an activity or event that can lead to the possibility of damage, harm or loss.

Risk assessment is fundamental for widespread commercial adoption, and risk management tools need to be integrated into the emerging Cloud paradigm.[25] While a variety of definitions of the term "risk management" have been suggested, in this work we adopt the definition given by the International Standards Organization (ISO) as follows: "a coordinated set of activities and methods that are used to direct an organization and to control the many risks that can affect its ability to achieve objectives."[26] This definition is close to the Black's Law Dictionary definition that refers to risk management as: "the activity of identifying, estimating and evaluating the probability of harm associated with an activity and determining an acceptable level of risk."[27] The underlying concepts of risk assessment and risk management aim to improve the confidence level between a provider and end-user to sign a SLA.[28]

---

[20]Non-functional requirements present a systematic approach that provides quality to the software system. They define the criteria used in the system operation, which is specified in the system architecture. For a comprehensive explanation of non-functional requirements see, e.g., Chung et al. (2000); Chung and Sampaio Do Prado Leite (2009).

[21]Li and Singh (2014), p. 670.

[22]"Clouds are a large pool of easily usable and accessible virtualized resources (such as hardware, development platforms and/or services). These resources can be dynamically reconfigured to adjust to a variable load (scale), allowing also for optimum resource utilization. This pool of resources is typically exploited by a pay-per-use model in which guarantees are offered by the Infrastructure Provider by means of customized SLAs." See Vaquero et al. (2008), pp. 50–55. The above definition is very useful because it also introduces a "customized SLA," which is explored in greater detail in this chapter.

[23]For this term see American Heritage Dictionary.

[24]Garner (2014), p. 1524.

[25]See, e.g., Gourlay et al. (2009), p. 36.

[26]Plain English ISO 31000:2009.

[27]Garner (ed) (2014), p. 1525.

[28]Sangrasi et al. (2012), pp. 445–452.

Risk assessment must be introduced proactively into the SLA framework to allow the end users and Cloud providers to automatically recognize critical points of failure (PoF), and to propose corrective actions that would reduce the risks in specific points of the contract in order to avoid soaring transaction costs and preventing future controversies. This precautionary approach is meant to fill in the gaps in the current SLA frameworks, and to imbue a risk management culture among Cloud providers.[29]

Despite the fact that many generic risk management assessment standards exist today such as the ISO 31000:2009,[30] one major difficulty that might arise in the implementation of this requirement is the lack of a standard risk assessment method for database rights and "ownership" rights of data. There are several risks and significant effort has been devoted to other areas of law such as privacy, data protection and data security.[31] For example the ISO 22307:2008[32] privacy impact assessment (PIA),[33] for financial services and banking management, the ISO/IEC WD 29134 PIA methodology,[34] the ISO/IEC 29101:2013 for information technology security techniques and privacy architecture framework[35] and the ISO/IEC NP 19086-4 for Cloud computing SLA framework still under development.[36]

The European Network and Information Security Agency (ENISA) released at the end of 2012 the updated version of its 2009 Cloud security risk assessment. The risks are classified into three categories: (a) Policy and Organizational, (b) Technical, and (c) Legal. It contains a list of 23 risks. One of these risks refers to intellectual property issues, which is a good indicator that the perceptions of associated risks of Cloud computing has put intellectual property rights (IPRs) under the radar. However, this is described, in our view, too broadly and focuses mainly on the copyrights of original work such as new applications, software, etc., while other aspects of IPRs such as database rights are not mentioned. As with all the IPRs described in the ENISA recommendations, database rights and other issues related to "ownership" rights of data must be clarified by the adequate contractual clauses and within the service manifest of the SLA otherwise this might be at risk. ENISA has played a crucial role in providing stakeholders an overview of the main

[29]See, e.g., Nwankwo (2014).

[30]ISO 31000:2009 risk management standard sets out the principles and guidelines on risk management that can be applied to any type of risk in any field of industry or sector.

[31]Cattedu and Hogben (eds) (2009).

[32]ISO 22307:2008 is a privacy impact assessment for financial services and banking management tools. It recognizes the importance to mitigate risks associated to consumer data utilizing automated and networked systems.

[33]See, e.g., generally, Corrales (2012), Wright and De Hert (eds) (2012).

[34]For details, see http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=62289. Accessed 10 April 2016.

[35]See ISO/IEC 29101:2013 Information Technology—Security Techniques—Privacy Architecture Framework; see also Nwankwo (2014).

[36]ISO/IEC NP 19086-4 Information Technology—Cloud Computing—Service Level Agreement (SLA) Framework and Technology—Part 4 Security and Privacy.

risks involved in Cloud computing and there is a second review round envisaged by the group of experts set up by ENISA where legal aspects will be revised in more detail as this was excluded from the first round.[37]

Until now, no systematic investigation has adequately explained database rights and "ownership" rights of data with consideration being given to the Cloud and Big Data phenomenon. In this regard, the present study is the first to undertake a specific risk analysis in this domain and aims to contribute to this growing area of research. Understanding the link between Big Data, database rights and "ownership" rights of data, will help to reduce the legal uncertainties and risks involved in Cloud transactions. Thus, the broadening of the scope of the risk assessment methods followed hitherto is accordingly designed and advocated in order to establish priorities and make strategic choices of Cloud providers a global reality.

Incorporating risk assessment techniques in Cloud brokerage scenarios and including database rights and "ownership" rights of data during SLA negotiations and service operation, will aid the decision-making process regarding contractual agreements. There is a current lack of confidence and trust in terms of the uncertainties involved with the SLA level of quality.[38] This is one of the most important barriers to the adoption of Cloud computing. In order to improve confidence and create more trust in Cloud transactions, it is necessary to improve control over the resources available. The design of Cloud architecture related to application deployment seems to be the best route to achieve this. This will also create more optimized and transparent resources.[39]

It is important to bear in mind that it is not possible to reduce all the risks down to zero. Nevertheless, mitigation strategies may at least increase the confidence of end-users and lead to a reliable productivity and cost-effective solution for Cloud service providers. In this research confidence is defined as "the expectation of a successful fulfillment of SLA agreed between a Cloud service consumer and a Cloud service provider,"[40] and the notion of cost-effective and reliable productivity as "a provider's capability of fulfilling an SLA through the entire lifecycle of the service provision and at the same time realizing its own business level objects of an SP."[41] In other words, capitalizing and making a certain amount of profit, while optimizing the efficacy of infrastructure provider resources.[42]

Based on the framework of the OPTIMIS[43] and AssessGrid software toolkits, as a basic risk factor mechanism, the main contributions of this research are the design and effective implementation of a risk assessment framework tailored to database rights and "ownership" rights of data with an eye towards Big Data and other future

[37]Dupré and Haeberlen (eds) (2012).

[38]Djemame et al. (2011a), p. 119.

[39]See, e.g., Kirkham et al. (2013), p. 7.

[40]Djemame et al. (2011a), p. 119.

[41]Djemame et al. (2011a), p. 119.

[42]Djemame et al. (2011a), p. 119.

[43]For details, see Ferrer et al. (2011), pp. 67–77.

similar movements. This can be efficiently implemented into other high-level Cloud management and control software systems for both service providers and infrastructure providers. Although a specific risk assessment is the main focus of this chapter, we also consider the decision-making process of how to implement corresponding mitigation strategies that may involve other high level considerations such as cost-efficiency and trust.[44]

3 Risk Assessment Methodology

Risk analysis can be examined at various stages of Cloud interactions. Each of the actors involved in the Cloud will have their own concerns and points of view towards others in terms of trust, risks and legal issues.[45] They might have specific legal demands that need to be taken into consideration. For example, how to reconcile the "ownership" of data that may accrue from the use of Cloud computing and Big Data technology? New data can be potentially created out of the data derived from the usage of various tools such data mining, analytics, AI, etc. The concept of "ownership" in this context implies that the owner can control how the data will be regulated.[46] Events like this and their impact need to be assessed in order to compute an overall probability of SLA violation, which requires a detailed analysis. This assessment will also depend on the Cloud deployment scenario—bursting, federated, hybrid, etc.[47] In this research we will consider a Cloud brokerage scenario since the broker can participate as an intermediary in any of these scenarios.

These legal concerns can also be refined considering the different stages of the Cloud lifecycle as follows: (a) the service deployment stage for initial placement of services on Cloud providers taking into account the legal issues as a gauge for Cloud provider selection, and; (b) the service operation, where Cloud resources and databases are managed by the Cloud provider for the attainment of all the service-level objectives (SLO), including the legal ones. During these two stages, legal risks need to be continuously and systematically monitored in order to avert any additional transaction costs to be incurred to the end-users and Cloud providers.[48] Figure 1 describes the risk assessment steps during service deployment and service operation.

A number of stages have been identified as a process with the aim of performing a complete risk assessment on Clouds. Each iteration is used to parse in real time, a

[44]Djemame et al. (2011a), p. 119.
[45]Khan et al. (2012), p. 122.
[46]Djemame et al. (2012), p. 3.
[47]Khan et al. (2012), p. 122.
[48]Khan et al. (2012), p. 122.

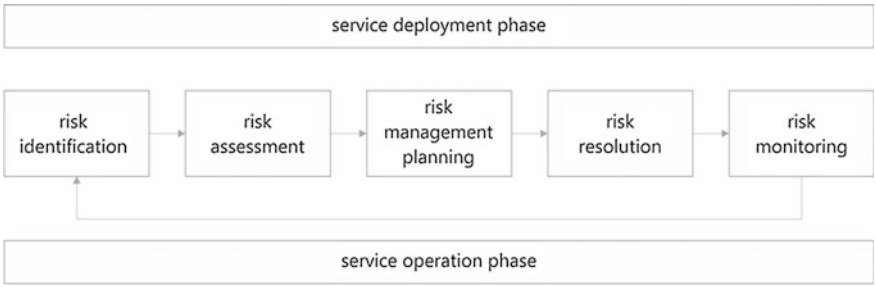

Fig. 1 Risk assessment life-cycle during service deployment and operation

core risk assessment and helps us to better understand the process. The constituent parts of this approach and their relationships are further explained below.[49]

3.1 High Level Analysis of the System

A primary high-level analysis of the different deployment scenarios aids identifying the actions and assets involved at different stages of the risk assessment process. This helps to effectively identify the vulnerable parts of each asset and how they can change through time. As a general rule, legal concerns need to be assessed before the service deployment phase if the SLA demands specific expectations to be met. In the service operation phase, the legal issues involved are constantly monitored throughout the service execution.[50]

3.2 Identifying the Assets Involved

There are various assets that need to be protected from specific threats during service deployment and operation phases. From a legal perspective, we refer here to data, databases and the terms specified in the SLA.[51]

3.3 Identifying the Threats in Each Cloud Deployment Scenario

The risk assessment model adopts a systemic approach by which threats and vulnerabilities can be identified. The risk analysis methodology is linked to a threat and

[49]Kahn et al. (2012), p. 122.
[50]Kahn et al. (2012), p. 122.
[51]Kahn et al. (2012), p. 122.

vulnerability assessment tool. This systemic approach is particularly helpful because it contains a threat model ensuring synergies with distributed systems and software in general. This model has been adapted to Cloud applications using the CORAS[52] risk modeling language technique, which is an open-source risk-modeling tool.[53]

4 Embracing Legal Risks and Enhancing Legal Interoperability

Richard Susskind, in his book *The Future of Law*, under the sub-heading: "From legal problem solving to legal risk management," anticipated a paradigm shift in the approach to legal problems. While solving legal problems will not disappear in the future, they will be substantially mitigated with proactive legal risk management tools and services that will pre-empt the conventional reactive legal method.[54] There is an increasing interest in the adoption of risk management methods borrowed from other disciplines that can be effectively adapted to use in the legal domain. Therefore, the proposed software-based risk assessment tools seem a reasonable preventive route for amending the legislative gaps and finding a solution for the many shortcomings of the rigid and unrealistic constraints of traditional black-letter laws.[55]

Preliminary work on legal risk management was undertaken as an approach to providing legal services in various areas of the IT industry and this continues to be an active area of research. However, these generic methods have not reached a high level of sophistication and have not been fully implemented yet.[56] Current software process optimized models do not properly address the legal implications for each phase of the software development lifecycle. The lack of systematic and organized standards in this domain provides only scattered references to legal aspects. This means that legal risks are managed reactively instead of proactively before damage or loss occurs.

Drawing on software projects, Rejas-Muslera et al., presented a significant analysis and discussion on the subject. The authors identified that legal audits are closely related to planning activities. According to Muslera et al., legal activities and measures must be planned in advance and invoked as time goes by across the entire lifecycle of the product or project in order to avoid or reduce negative legal impacts on the achieved objectives. Despite their study covers many aspects of law, including copyright, registration and user's rights, data protection, trading

[52]See, e.g., Vraalsen et al. (2005), pp. 45–60.

[53]Kahn et al. (2012), p. 123; Djemame et al. (2012), p. 12.

[54]See Susskind (1998), p. 290.

[55]Wahlgren (2007), p. 91; See also Wintgens and Thion (2007), Introduction.

[56]Burnett (2005), pp. 61–67.

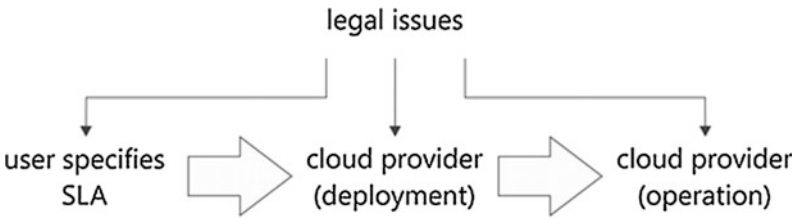

Fig. 2 Legal issues and service life-cycle stages

standards, etc.,[57] the core interest of the present research lies in the risks associated with managing databases.

The main goal is not to deny these risks and their overall implications but to create a smart strategy than can deal with this trade-off. In the following sections, we discuss these legal aspects in the context of Big Data and Cloud computing. Legal issues are present at each phase of the whole outsourcing life cycle of a Cloud service. Figure 2 shows a graphic depiction of the overall model from a high-level perspective:

In the initial contractual agreement stage, the end-user may specify legal clauses with regard to certain service requirements and how such databases must be handled. While large companies and institutions may have more resources to bargain and negotiate specific contractual clauses, the standard nature of the SLAs do not allow much room for single users and SMEs to negotiate the contract.[58] However, an XML automated schema[59] has been specifically crafted to provide more flexibility for smaller companies and individuals so they can clarify database rights and "ownership" rights of data, and all parties involved can be better off. Nevertheless, the point to bear in mind for the moment is that notwithstanding the negotiation capabilities of end-users, these contracts are legally binding. The Cloud provider must fulfill all the requirements and ensure that all clauses will conform to legal rules before deploying the service. Otherwise it will be at risk of facing liability issues should there be any breach of the contract. Therefore, monitoring strategies of legal risks should be present throughout the operation phase.[60]

[57]Rejas-Muslera et al. (2007), pp. 118–124.

[58]Bradshaw et al. (2010).

[59]XML is a markup language standard that aims to define a format that is both human and machine understandable. Thus humans based on a template model may edit it, and the produced created instance can be processed by according software, following a relevant decision logic. For example, the template model dictates the available fields, the user selects the according values, and then the relevant software may retrieve the XML-based provider descriptions and filter them based on the user's requirements. The XML Description Schema is available at: http://www.optimis-project.eu/content/xml-description-schema-improvement. Accessed 10 October 2016. For details about the XML schema see previous chapter.

[60]Batré et al. (2007), p. 193.

This framework will improve the legal interoperability among providers on a global scale. According to the GEO Data Sharing Task Force, legal interoperability among multiple datasets from different sources occurs when: "the legal rights, terms, and conditions of databases from two or more sources are compatible and the data may be combined by any user without compromising the legal rights of any of the data sources used." [61] This definition is important for what it includes as the following conditions[62]:

(i) The conditions to use data are clear and readily determinable for each dataset[63];
(ii) The legal conditions granted to use each dataset permits the creation and use of "combined and derivative products,"[64] and;
(iii) End-users may lawfully get access and use each dataset without seeking permission from data creators.[65]

Legal interoperability is a bottleneck in Cloud computing transactions, where many resources are available and data is used, re-combined and then derivative data is re-disseminated. This might also prove a great hindrance to public research. The protectionist mentality underlying database rights is, however, very dangerous because it automatically frames access to data as a threat. Within this mindset, there is a risk of databases being locked in. As we shall see soon, the database rights (sui generis right) casts serious problems on the Big Data movement, which does not understand the protection of databases in the same way as the protectionist mentality. The quest for Big Data invites the researcher or entrepreneur to a place where information can lead to innovation and productivity. There should be an equitable trade-off between the protection of databases and access to data that is in the public domain.

The term public domain has come to be used to refer to "information that is: (a) not subject to copyright or related rights (including database rights), and; (b) not subject to conditions on reuse imposed by other means."[66] This approach could raise and promote social welfare and the goals intended by the Big Data movement by making datasets available to end-users. In a free market economy individuals should be allowed to obtain unrestricted use and re-dissemination of data. This market competition process may help to correct behavioral market problems. The public domain status may be created formally through laws and policies that exempt

[61]For details, see Draft White Paper on Legal Options for the Exchange of Data through the GEOSS Data-CORE. Group on Earth Observations.

[62]White Paper, Mechanisms to Share Data as Part of GEOSS Data-CORE, p. 3.

[63]White Paper, Mechanisms to Share Data as Part of GEOSS Data-CORE, p. 3.

[64]White Paper, Mechanisms to Share Data as Part of GEOSS Data-CORE, p. 3.

[65]White Paper, Mechanisms to Share Data as Part of GEOSS Data-CORE, p. 3.

[66]Summary White Paper, Legal Options for the Exchange of Data through the GEOSS Data-CORE, p. 2.

certain categories of data and information from database protection. However, this could also be achieved through contractual private agreements among parties.[67]

For many scholars, the database right is considered unsuccessful. The detractors of the EU Database Directive have often expressed the criticism that this could be raising hurdles to innovation and free development in various areas of industry.[68] Another objection to database rights is that this may lock up data and information, which can negatively affect the research and academic community that rely on the availability of data and information to carry on their business or research.[69] According to Kingston, the EU Database Directive has been influenced by publisher lobbying, which confers them the potential to attain a continuous monopoly on data.[70] Quoting the words of Reichman and Samuelson, the database right is "one of the least balanced and most potentially anti-competitive intellectual property rights ever created."[71] Finally, opponents of these rights argue that this form of protection is too narrow in scope and fails to address other relevant issues for the database industry.[72] These arguments clearly show the negative perception among some scholars, which prompts worries about its potential negative effects.

It is not the purpose of this research to enter into such controversies. Nevertheless, we would generally agree with the idea that database rights could potentially distort the right to access information and certain issues of abuse of monopoly could emerge, in particular if one look at this problem from a global Cloud computing perspective. We think all these arguments are legitimate and that sui generis rights could eventually lock up data to the detriment of the scientific and academic community as well as other areas of industry. This yields much greater protection to databases, yet with a certain degree of uncertainty that may fall foul of prior intellectual property law principles by placing strong exclusive property rights on investment instead of creativity and innovation. Still, we find it possible to argue for a more balanced approach, which is more flexible and less objectionable than database rights. In order to respond to the critics of sui generis rights, what we propose is a mechanism that follows the core principles and guidelines of best practices through which legal interoperability, and, a right balance between the transferability of conventional databases and the availability of Big Data can be achieved.

---

[67]Summary White Paper, Legal Options for the Exchange of Data through the GEOSS Data-CORE, p. 19.

[68]Sundara Rajan (2011), p. 286.

[69]For the extensive case law on this topic see, e.g., Fixtures Marketing Ltd. v Oy Veikkaus AB, CJEU—Case C-46/02, 9 November 2004 (Finland); Fixtures Marketing Ltd. v Organismos Prognostikon Agonon Podosfairou [the OPAP case], CJEU—Case C-444/02, 9 November 2004 (Greece); Fixtures Marketing Ltd. v Svenska Spel AB, CJEU—Case C-338/02, 9 November 2004 (Sweden); The British Horseracing Board Ltd and Others v William Hill Organization Ltd., [the BHB case], CJEU, Case C-203/02, 9 November 2004 (United Kingdom).

[70]See Kingston (2010), p. 112.

[71]Bently and Sherman (2009), pp. 310–311.

[72]DG Internal Market and Services Working Paper, First Evaluation of Directive 96/9/EC on the Legal Protection of Databases, p. 4.

5 Conventional Databases Versus Big Data: Striking the Right Balance

As seen above, the sui generis right is a well-established IPR protected under the umbrella of the EU Database Directive. This right stems from the necessity to foster the database industry in the EU in a time where databases needed an extra scope of protection.[73] However, this right caused some concerns and uproar among legal experts, mainly due to its failure to come to terms with new technological advances of the Internet and with the onset of Cloud computing services along with the Big Data movement, which may undermine and hamper scientific and research activities.

The Database Directive is still clinging to old-fashioned ideas of conventional databases that have a fixed structure on which one accumulates and stores data. Another defining factor is the ubiquitous nature of the Cloud that often obscures the physical location of databases. The ability of Cloud providers to transfer databases across multiple countries represents the problem of dealing with different legal jurisdictions. This situation can collide with the legislation of those countries where database rights do not even exist. Therefore, the first problem to be addressed in the contracts is that database rights should only be implemented in jurisdictions where this right exists and limited to a geographic location due to its territorial nature.

We think that this represents a good starting point. However, if we follow this approach only, this debate continues to be stuck in the old paradigm. In view of the immense influence of the Big Data phenomenon, the real issue lies elsewhere. If our aim is the empowerment of end-users so they can take the initiative and make decisions in the face of the Big Data movement, then database rights seem entirely counterproductive. The explosive growth[74] and breadth of reach of Big Data has expanded so much that it has surpassed the traditional logistics of storing, processing, or analyzing data.[75] It touches upon almost every corner of the digitized world and its benefits have enthralled all aspects of human life.[76]

Nevertheless, this great exposure comes along with various risks and opens the door for litigation.[77] Big Data in the Cloud refers not only to the storage and accumulation of large amounts of data but also how to organize and label such data

[73]The concept of protecting databases with only copyright changed radically right after a series of case laws rejecting copyright protection such as the *Van Daele v Romme* ruling in the Netherlands, where Van Daele could not protect the copying of its dictionary because of lacking the threshold of originality, and; the *Feist Publications v Rural Telephone Service Co.* [*Feist* case] judgment in the US, where the courts decided not to grant copyright protection to a phone directory on the same grounds. See Van Dale Lexicografie B.V. v Rudolf Jan Romme, Hoge Raad, Supreme Court of the Netherlands, 4 January 1991, NG 1991, 608 (The Netherlands); Feist Publications v Rural Telephone Service Co. 499 U.S. 340 (1991) (United States).

[74]Majkic (2014), Preface.

[75]Dean (2014), p. 10.

[76]Ridley (2015), p. 79.

[77]Ridley (2015), p. 79.

in a variety of different and useful ways[78] (structured, unstructured,[79] semi-structured,[80] etc.). Big Data generally slices and dices information. This breakdown process implies a systematic reduction of information into smaller pieces that can be arranged in a way that will yield new information. This includes machine-generated data from automated sensors, nuclear plants, X-ray and scanning machines, airplane engines, consumer interaction from businesses,[81] mobiles and social media.[82] If this information is exploited properly it will revolutionize the decision-making process—entrusting more on data analysis instead of intuition and experience. This being said, individuals and institutions need to consider not only the best means to generate and exploit data but also how to protect and manage their data. This raises challenging questions about policies and practices that have direct implications on our lives.[83]

The vexed question is how to strike the right balance between the *transferability* of conventional databases and the *availability* of Big Data. This research attempts to answer some of these lingering questions and fill a long-held gap in the scientific literature. In line with the principle of free and open access to data,[84] the framework we propose endows end-users and Cloud providers with a flexible mechanism through the Cloud broker to ensure freedom of contract. This interpretation gleaned from the aforementioned principles and ideas can best be treated under three headings: (1) Territorial scope of protection, (2) "Ownership" rights of new data generated by the Big Data movement in the Cloud, and; (3) Lack of international legal and contractual standards, as follows:

5.1 Territorial Scope of Protection

This problem relates to the ubiquitous nature of the Cloud and the territorial scope of protection of database rights that creates legal hurdles. One of the most contentious provisions of the EU Database Directive, which is relevant to our discussion, in particular in the context of Cloud computing and Big Data, is Article 11 which establishes territorial constraints with regard to who may be subject to obtain database rights. In principle, the right extends only to makers or rights holders who are nationals or habitual residents of a EU Member State. This is further explained

[78]See, e.g., generally, Sakr and Gaber (eds) (2014).

[79]Unstructured data is the subset of information. For example: text mining in the medical field. For details, see, e.g., Holzinger et al. (2013), p. 13.

[80]Semi-structured data such as XML. See, e.g., generally, Ishikawa (2015), Kitchin (2014).

[81]Krishnan (2013), p. 5.

[82]Vashist (2015), p. 1.

[83]Lohr (2015).

[84]See, e.g., generally, OECD Principles and Guidelines for Access to Research Data from Public Funding (2007).

in Article 11 (2) that includes companies or firms, which have their principal place of business or central administration within the EU.[85] This is a controversial and anachronistic provision in the context of Cloud computing and Big Data due to its essentially pervasive nature. In view of the fact that servers can be located in different countries outside of the EU, and that databases can be easily reproduced in virtual machines (VM), there is a risk of potential future controversies between the parties involved in Cloud computing transactions.

If a database qualifies for protection, and it is stored on a server, which is within the jurisdiction of EU/EEA Member States, then there is no doubt that it will be protected. However, the crucial question to determine here is whether the jurisdiction applies to the place where the database has been created or where the database has been recorded. This distinction will fundamentally affect database protection in Cloud transactions, as there are no database rights in other countries outside of the EU.[86]

Currently, there is not such an automated procedure for checking whether database rights are clearly defined and specified so that a broker can "on the fly" confirm the legal compliance. These checks may include the location of the federated infrastructure provider using a location constraint mechanism. If the target infrastructure provider is inside the jurisdiction of the EU/EEA Member States then the outsourcing of data and databases may be fulfilled with minimal intervention taking into account that database rights exist within the jurisdiction of European countries. If the infrastructure provider is located outside the boundaries of any of the EU/EEA Member States, and, therefore, outside of the scope of the Database Directive, then the federation cannot be performed if these checks are not in place in advance.[87]

However, Cloud customers can decide to waive their database rights in order to federate the databases outside the boundaries of the EU/EEA Member States. As seen earlier, databases represent the risk of being potentially "exported" overseas to a jurisdiction without database rights. Therefore, they should only be implemented in jurisdictions where this right exists and limited to a "geographic location" due to its territorial nature. For this reason, we propose a legal "glocalizational"[88] solution that includes an unconditional waiver as an alternative for scientific databases and/or for databases transferred across different jurisdictions outside the EU/EEA countries.

[85]Davison (2003), p. 97.

[86]With the exception of Mexico, South Korea and Russia.

[87]See, e.g., Kousiouris et al. (2013), pp. 61–72. In this work, the authors refer mainly to data protection issues, however the same principles and ideas underlying the geographic location and data transfers could apply to database rights.

[88]According to Annupan Chander, legal glocalization "would require the creation or distribution of products or services intended for a global market but customized to conform to local laws—within the bounds of international law." See Chander (2013), pp. 11, 16, 137, 143, 144, 145 and 169.

5.2 *"Ownership" Rights of New Data Generated by Big Data*

As hinted above, the exponential growth of data, both structured and unstructured, and the booming of Big Data trends, have the ability to create new information from the data submitted to the Cloud. This newly created data has value for both end-users and Cloud providers. This means that some of the provisions enshrined in the EU Database Directive are becoming obsolete. Furthermore, there seems to be a lack of international legal standard that defines "ownership" rights of data accruing from scientific research and Big Data analyses. There is some sort of prevailing "global norm," where the person or company who collects the data, "owns" it. This problem seems to bring conflicting arguments between the involved parties. Therefore, there is a need for an efficient and automated procedure during the negotiation of SLAs in Cloud computing transactions, which aims to establish a clear and effective procedure to layout early in the contract who "owns" this data and define the conditions as to whether data will be shared or not among, for example, Cloud providers and end-users, researchers/doctors and patients, etc.

5.3 *Lack of International Legal and Contractual Standards*

The third problem is the lack of a common international contractual framework to mitigate these legal risks. This leads to a lack of interoperability at the global scale that obstructs the Cloud computing and Big Data markets from thriving. Cloud customers are facing difficulties in choosing the right Cloud provider that best fits their needs. The lack of a structure or frame supporting the clarification of such rights creates tension between the stakeholders involved in Cloud computing transactions. Customers using Cloud computing services are not longer satisfied to deal with these uncertainties post facto. They need clear guidelines at the time they enter into a Cloud computing transaction.

As a corollary, due to the lack of an efficient and automatic procedure for the clarification of database rights and "ownership" rights of data in the Cloud, end-users have to cope with the uncertainties and intricacies of the decision-making. The current state of the art in the Cloud market allows only for a limited category of static and non-negotiable click-through SLA (usually ranked as gold, silver, or bronze). The manual selection of Cloud providers in order to meet their functional requirements (e.g., storage capabilities, number and size of servers, etc.) and non-functional capabilities (e.g., legal) has been perceived as imposing transaction costs. End-users must go through the cumbersome procedure of visiting manually the websites of Cloud providers to compare their quality of services and legal policies.[89]

[89]See Wu et al. (2013), pp. 235–244.

In short, what we want to achieve is a flexible and automated SLA that includes: (i) the possibility to keep databases (and as a consequence database rights) within the EU jurisdiction.[90] This would be the case an end-user does not want to share data and still keeps database rights and enjoy the benefits of the EU Database Directive. If so, databases should stay within the EU jurisdiction; (ii) the possibility to clarify who "owns" the processed and derivate data. This would be the case of Big Data projects/applications, e.g., using data mining tool techniques, statistics, analytics, etc., where there is potentially valuable information for both the end-users and Cloud providers. The contract should be able to clarify who "owns" this new data. This situation is between end-users and providers, or potentially among end-users working in the same project e.g., a research project using genetic, geo-data, spatial data, etc. It goes without saying that all these legal issues could be clarified via a consortium agreement (CA). In a realistic Cloud computing scenario, however, what we need to avoid are manual negotiations. Therefore, this capability should be carried out automatically, and; (iii) a waiving mechanism, by which end-users may relinquish their database rights and "ownership" rights of data. This would be the case of a Big Data collaborative project where many countries are involved.[91] This way databases would remain open and everyone could get access and tap into it. On the one hand, most research is conducted by joint efforts of public as well as private institutions in interdisciplinary and international contexts. On the other, competition in a behaviorally imperfect market is inevitable, and the possibility of waiving database rights does not mean that competition has to be curtailed. Providing more information and warning signals can offer end-users more choices and grant them more control over their data.

6 Risk Assessment Techniques and Typical Actors Involved in Brokering WS-Agreements

This section focuses on explaining in more detail the brokering mechanism, which facilitates the creation of risk-aware SLAs between the typical actors involved in Cloud computing transactions. Three actors exist in the architecture of a typical Cloud brokerage scenario: end-user, broker and provider. An end-user is an individual or a company who wants to use the Cloud in order to perform certain task consisting of one or more services. The user must explicitly specify the tasks and associated requirements within an SLA template. In the preamble of this process, the end-user needs to make informed and risk-aware decisions on the SLA quotes. In order to make this risk assessment more practical, we consider two broad typical brokerage scenarios that provide ideal use cases. In both situations resources are dynamically allocated and redistributed. These scenarios are the following:

[90] Or, for example, in Mexico, South Korea and Russia as these countries have also database rights similar to the EU Database Directive.

[91] See, e.g., GEOSS-data Core project, p. 11.

(a) *Broker as Mediator*: In this case the broker performs a risk assessment on behalf of the end-user in order to find the most suitable Cloud provider and bring the parties together. It follows a four-step process: First, the end-user sends an SLA request to the broker. Then, the broker forwards the SLA quotes to a pool of suitable Cloud providers. Once all the SLA quotes are received from the providers, the broker performs an independent risk assessment of each provider. Then, the broker creates a ranked list according to their PoF. Finally, the end-user is then free to choose and commit to an SLA quote by engaging directly with the selected provider.[92]

(b) *Broker as Contractor*: In this case the broker takes a more active role and offers its own SLA to end-users. The risk assessment works in the same way of the previous scenario. However, the main difference here is that the broker takes full responsibility of the SLA and performs the role of a "virtual" provider. Therefore, an end-user contracts directly with a broker instead of with the Cloud provider. The broker agrees to the terms and conditions of the SLA between itself and each Cloud provider.[93]

This brokerage mechanism will be used as a technical framework to include database and "ownership" rights of data risk assessment techniques. It is in the best interest of both sides: (a) end-users: as it increases the selection of Cloud providers by comparing SLA quotes that match their expectations, and; (b) Cloud providers: as it generates a larger user pool base and attempts to reduce deliberation costs in deciding upon which SLA requests to accept. From a provider's perspective, accepting an SLA implies the potential risk of paying a penalty if such commitment cannot be met.[94]

It is important to bear in mind the limitations of this framework. The introduction of a broker alone will not dissipate all the uncertainties before signing the SLA. Nonetheless, the implementation of a risk-aware brokering mechanism provides the means to formally evaluate the probability and expected impact of potential adverse events. Without such knowledge end-users and Cloud providers cannot take the right decisions with regard to costs and benefits. In a nutshell: this is a win-win situation that will reduce transaction costs.[95]

Nevertheless, the crucial question that remains is whether the Cloud brokers are poised to offer a viable and transparent alternative route for end-users and Cloud providers.[96] To some extent the Cloud broker-enabling technology should improve the available choices by providing the means for control and transparency to make effective and proactive data-driven decision-making.[97] From the perspective of

[92]Djemame et al. (2011b), p. 1561.
[93]Djemame et al. (2011b), p. 1561.
[94]Djemame et al. (2011b), p. 1561.
[95]Djemame et al. (2011b), pp. 1559–1560.
[96]Fellows (2013); see also Gourlay et al. (2008), p. 438.
[97]Fellows (2013).

end-users, the broker should be seen as a trusted advisor that aids them to make better decisions.[98]

For this reason, a relevant aspect of this framework is the implementation of a software component—a *confidence service*; designed to perform an independent and objective assessment of the reliability of Cloud providers in relation to the SLA PoF. Cloud providers usually run their own risk assessment, however, this can be too optimistic and overlook some of the important facts that are relevant for end-users. Therefore, the confidence service component provides more transparency and additional risk information to enhance the SLA decision-making process of end-users.[99]

7 Risk Inventory Design

Designing a risk inventory depends on the purpose and area in which they are applied. It has to be contextualized taking into account all the parties involved. As explained above, in our use case scenarios, these actors are end-users, Cloud providers and the broker who can acquire different roles (mediator or contractor).[100] The risk inventory may also have different categories. In the case of the OPTIMIS risk assessor component, there are four broad categories i.e., general, technical, policy and legal.[101] A risk inventory must be tailored and refined to fit a specific purpose. For the implementation of this framework, a set of processes has been identified as follows[102]:

(i) *Use cases*: determine precisely which use case scenario to focus on: in this case, a Cloud brokerage scenario[103];
(ii) *Levels of interaction*: establish the areas of interaction in the Cloud. Interactions may involve various levels in the Cloud. In this case, we consider two levels: (a) end-user to service provider, and (b) service provider to infrastructure provider. Insomuch as during each of these levels particular aspects of the SLA needs to be agreed upon and its fulfillment monitored[104];
(iii) *Assets*: it is necessary to identify what is the asset being protected. In this case, database and "ownership" rights (and their characteristics) and SLAs. Risks events will be assessed and protected taking into account external or internal dangers (risks)[105];

[98]Fellows et al. (2014), p. 2.
[99]Djemame et al. (2011b), pp. 1559–1560.
[100]Djemame et al. (2011b), p. 1561.
[101]Djemame et al. (2011a), p. 122.
[102]Djemame et al. (2012), pp. 9–10.
[103]Djemame et al. (2012), pp. 9–10.
[104]Djemame et al. (2012), pp. 9–10.
[105]Djemame et al. (2012), pp. 9–10.

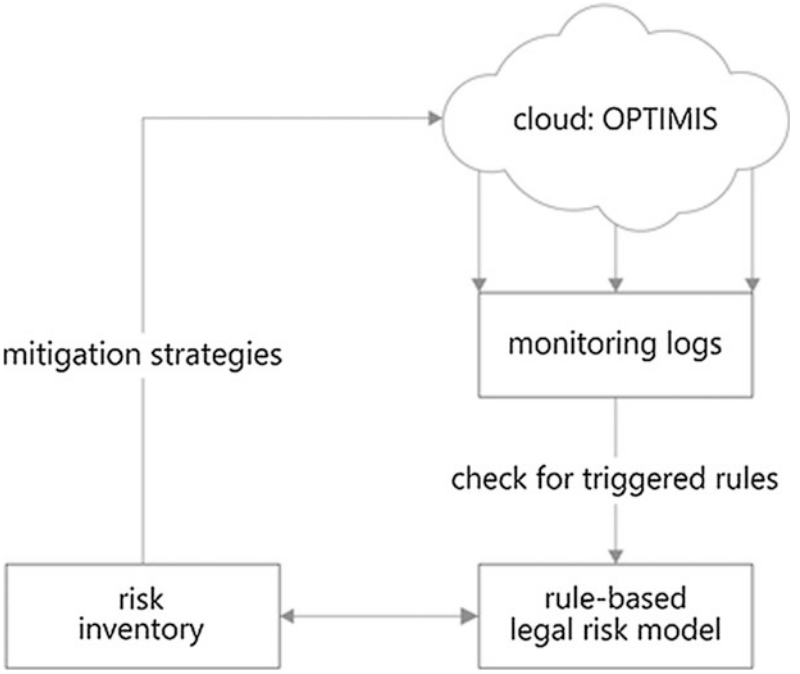

Fig. 3 Risk inventory for the identification of legal risks in the cloud architecture

(iv) *Incidents/Risk Scenarios*: it is necessary to describe any event, condition or a blend of both that has the potential to diminish the capacity or availability of an asset. These consist of the vulnerabilities and threats these assets may have during service operation. This includes the "adaptive capacity," which is the specific description of the mitigation strategy to be carried out for each risk scenario and its asset[106];

(v) *Triggering Factor*: it is necessary to identify the factors that lead to activate risk. Risks may also be dynamic. This means they can change and continually fluctuate over time as they are directly exposed to changes in the Cloud ecosystem such as regulatory requirements, changes in policies and contractual clauses, transactions, etc. The implementation of monitoring strategies may help to mitigate them during Cloud service deployment and operation phases.[107]

[106]Djemame et al. (2012), pp. 9–10.
[107]Djemame et al. (2012), pp. 9–10.

The risk inventory designed within the scope of the OPTIMIS project has been integrated as a rule-based legal risk[108] modeling component and an integral part of the risk assessment software tool (see Fig. 3). The risk assessment tool is a "self-contained independent functional model," which means that it is a completely independent component that enables customization and is able to work as a "plug-in."[109] This allows the addition of specific features to the existing software application. In the context of the OPTIMIS toolkit, the risk assessment tool has been implemented as two coexisting but independent components as follows: (a) the service provider risk assessment tool (SPRAT), and; (b) the infrastructure provider risk assessment tool (IPRAT).[110]

8 Different Stages of Risk Assessment in Cloud Brokerage Scenarios (CBS)

As explained earlier, in a typical CBS there are three main parties involved. These are, the end-users, the broker and the Cloud provider. The Cloud provider could be a service provider or an infrastructure provider (i.e., virtual machine (VM) provider). From a service and infrastructure provider perspective, data management services are supplied by the broker to co-ordinate and provide services or infrastructure in terms of data processing and quality of service. Figure 4 shows the document flow for creating an SLA and the different stages where the risk assessment can take place. This procedure takes part during the whole service life-span (establishment, deployment and execution phase).[111] With a view to making it easier for the layperson, this process can be split into five consecutive steps as follows:

(i) At stage number 1, the SLA request is sent to various infrastructure providers (e.g., IP A, IP B, and IP C). At this stage, the broker wants to know which provider can run a service upon end-user's request. Prior to making this contact the broker should be able to assess the end-user's requirements and "filter" from its list of infrastructure providers those that may be able to make an SLA offer. Note that upon receiving an SLA request the infrastructure

[108]In computer science and software development, rule-based systems (also known as "expert-systems") are used to store and analyze information in useful ways that tell you what to do in different situations. They are often used as the basis for AI programing and systems to find answers to various problems. See, e.g., generally, Grosan and Abraham (2011), pp. 149–185; Toosizadeh and Reza Farshchi (2011). Rule-base systems work as a set of "If-then" rules and facts to represent different actions to take. For details, see Cawsey. Rule-Based Systems. http://www.zemris.fer.hr/predmeti/krep/Rules.pdf. Accessed 10 Oct 2016.

[109]Plug-in, add-in or add-on extensions are all synonyms for software components.

[110]Djemame et al. (2011a), pp. 121–122.

[111]Kirkham et al. (2013), p. 1067.

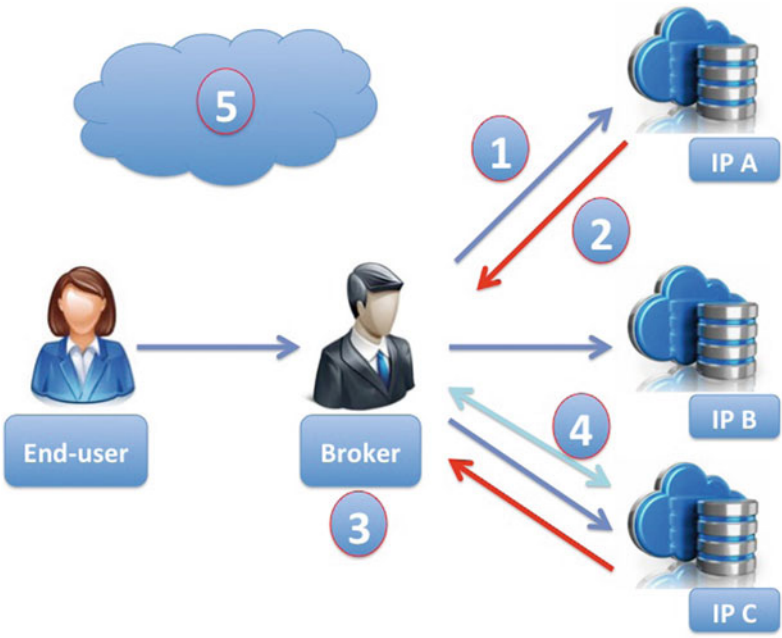

Fig. 4 Different stages of risk assessment in CBS

provider can selectively choose to accept it (and consequently the SLA needs to be fulfilled at service operation) or reject it;

(ii) At stage number 2, the broker receives a reply from the infrastructure provider in the form of an SLA offer. It may happen that the broker will receive several replies from different infrastructure providers. In Fig. 4, the broker receives an SLA offer from IP A and IP C;

(iii) At stage number 3, the broker *filters* all the offers received from the infrastructure providers who can run the service. At this stage, the broker can see which offer is more favorable to the end-user, i.e., proceeds with a *ranking*;

(iv) At stage number 4, the broker selects the most suitable infrastructure provider among all the SLA offers and contracts with one of them. At this stage, the SLA is bound between the infrastructure provider and the broker;

(v) At stage number 5, the service is in operation. At this stage, the broker has chosen and told the infrastructure provider to run the service.

Risk can occur at any time. That is, at stage 1, risk can take place before sending an SLA request to the infrastructure provider. In this case, the risk assessment is going to assess the risk of *dealing* with various infrastructure providers. This will work as a kind of "pre-assessment" when the broker is about to choose the provider.

After this first screening procedure, the broker can then discard the providers that do not comply with the end-user's requirements. At stage 3, the broker *filters* the provider's offer. In this case, the risk assessor component can "look" inside the shortlisted SLA offers and can assess the risk of *accepting* the SLA. At stage 5, the infrastructure provider is running the service. Therefore, the risk assessor component assesses the risk of the SLA *failing* during service operation. These are all different kinds of risk assessments. In addition, the risk assessment is from both sides as it can be run by the broker on behalf of the end-user and by the infrastructure provider. In the latter case, the infrastructure provider might have the same questions i.e., what is the risk of *dealing* with this broker? What is the risk of *accepting* this SLA request? And, finally, what is the risk of the SLA *failing* during service operation?[112]

The question arises, what does this all have to do with databases and the "ownership" rights of data? The reason is that all of the above could be tailored to database rights and "ownership" rights of data. It could be an integral part of the equation, i.e., part of the SLA negotiations. A key point of this research is to extend the scope of parameters and the range of conditions that can be understood, measured and evaluated. This needs to be included in the risk assessor model as an extension to the legal category. Database rights and "ownership" rights of data can be part of the "policy," "legal," "technical" and "general" criteria to be considered and evaluated. For instance, what is the risk of dealing with an infrastructure provider considering database rights? To answer this question, one may look at different criteria that can be assessed *quantitatively* or *qualitatively*. These criteria can refer to different areas that have been filtered from the ISO standards[113] and ENISA guidelines such as: back SLA performance, business stability, general security practices, privacy practices, certification standards, geographic location of the infrastructure providers, general infrastructure practices (e.g., information about back-up, history, machine, etc.)[114]

A *quantitative* risk assessment provides a numerical expression of probabilities.[115] It is based on track records of the broker dealing with the infrastructure provider. It is a reputation-based mechanism that classifies information based on past SLA performance. A risk level numerical estimation can be used to represent the probability of a risk that a specific harm will result from the occurrence of a particular event. For example, a 10-point rating scale: from 10 times, the infrastructure provider fails 1 time. The score is 9 out of 10.[116] Travel websites such as Trip Advisor are clear examples of this kind of ranking system. They often provide a forum where previous travellers can share their opinions and experiences.[117]

[112]Djemame et al. (2011a), p. 125.

[113]See, e.g., ISO 31000:2009; ISO 27000 standards; ISO Guide 73:2009.

[114]For details of the ENISA Guidelines see Cattedu and Hogben (2009).

[115]Summer et al. (2004), p. 6.

[116]Djemame et al. (2011b), p. 1570.

[117]Lebber and Hermann (2013), p. 406.

The data is analyzed within the inherent reputation engine of the risk assessor model using algorithms and statistical analysis. This score is then translated into the risk. The highest score represents a high risk and lowest score a very low risk. This forms part of the "confidence service" that has been developed as part of the risk assessment model.[118] The only downside to a quantitative reputation-based risk assessment is when there are no track records, i.e., when there is no past-SLA information. In this case, the information has to be garnered from scratch. Stages number 1 and 3 in Fig. 4 are relatively easy as they refer to existing data, i.e., data that has already been collected.

Stage number 5 is, however, more difficult to calculate, as this data has to be interpreted semantically and needs to be collected when the service is running during service operation. At this stage, the approach of any risk assessment must be *qualitative*. This method is conditioned to prior expert knowledge based on non-numeric values.[119] This means that the information or data that needs to be collected are expressed in verbal form instead of numbers or quantities as in the case of the quantitative method.[120] Therefore, the risk inventory must be extended to support database rights and "ownership" rights of data either as a new category or as part of the legal risk criteria. The qualitative risk assessment model needs data to be monitored based on the *vulnerabilities* and *threats* attached to it. This becomes one more component at the moment of assessing the overall risk of the SLA failing at the service operation phase (e.g., the risk of a computer system or VM failing in cases of natural disasters such as earthquakes, floods, etc.)[121]

9 Use Case Scenario: Examples

In this section, a hypothetical scenario is considered to showcase how the risk assessment can be effectively applied in real cases with an emphasis on the different threats and vulnerabilities identified as in the risk assessment process. To address these legal issues, we need to envisage a hypothetical scenario where database rights and "ownership" rights of data are breached or likely to be breached. For example, if the right to access a database has been granted, what are the inherent risks of that happening? Or, if database rights have not been granted, what are the results of this happening? In other words, we need to identify the specific *threats* and *vulnerabilities* related to database rights and "ownership" rights of data. Note that a threat is "a potential cause of an unwanted incident,"[122] which may cause harm to a system or organization,[123] whereas a vulnerability is "a weakness, flaw or

[118]Djemame et al. (2016), p. 3.
[119]Taubenberger et al. (2011), p. 260.
[120]Sharif and Basri (2011), p. 222.
[121]See, e.g., Cayirci (2015), p. 163.
[122]Lund et al. (2011), p. 131.
[123]Luiijf (2016), p. 69.

Table 1 Risk exposure rating

Likelihood	Impact				
	Negligible	**Minor**	**Moderate**	**Major**	**Extreme**
Rare	Low	Low	Low	Medium	Medium
Unlikely	Low	Medium	Medium	Medium	High
Possible	Low	Medium	Medium	High	High
Likely	Medium	Medium	High	High	Very high
Almost certain	Medium	High	High	Very high	Very high

deficiency that opens for, or may be exploited by, a threat to cause harm to or reduce the value of an asset,"[124] e.g., the database and the right to access it. It is only then when the obvious gaps are realized and the risk assessment model acquires its full value, as we will have a better understanding of the concrete data that we need to assess, measure and monitor in those situations and convert it into a specific risk analysis, risk being "the likelihood of an unwanted incident (an event) and its consequence (impact) for a specific asset."[125]

"Several consequence descriptors may apply to a single risk. The most serious/significant of these should be used to determine the risk exposure rating. The likelihood and impact levels are then cross-tabulated to give a risk exposure rating."[126] This calculates whether a risk is ranked as low, medium, high or very high (see Table 1).[127] This ranking of risks, that are assigned the same risk exposure rating, is determined by examining the strength of the control measures in place for these risks. For instance, "a *high* rated risk could have effective control measures in place that cannot be improved upon, whereas a *medium* rated risk may not have any control measures in place, and this is the risk that should be prioritized for action."[128]

We focused on a hypothetical scenario targeting a broad sector within the scope of a globalized world. This use case scenario refers to a research form that is typically found in transnational research such as genetic research projects within

[124]Großmann and Seehusen (2016), p. 23; Lund et al. (2011), p. 137.

[125]Beckers (2015), p. 457.

[126]Lund et al. (2011), pp. 121 et seq.; see also, e.g., The risk management of HAI: A Methodology for NHSs available at: http://www.gov.scot/Publications/2008/11/24160623/3. Accessed 10 January 2017.

[127]Use of colour coding could also facilitate the rapid communication and understanding of risks such as: red, amber, yellow or green.

[128]Lund et al. (2011); The risk management of HAI: A Methodology for NHSs available at: http://www.gov.scot/Publications/2008/11/24160623/3. Accessed 10 January 2017.

clinical trials. In this context, the risk assessment model is combined with an adaptive and flexible SLA with a data centric monitoring infrastructure. The main focus is to expand the range of SLAs to cover cross-border activities similar to the use case depicted below. The outcome is a contribution to equip the involved parties with a tool that can offer more choices to satisfy the legal requirements in Cloud computing and Big Data transformations.

9.1 Use Case Scenario: Genetic Research Projects Within Clinical Trials

Genetic research projects within clinical trial scenarios frequently collect biological and genetic data from patients/participants. This data is then stored in a hospital's databases for future research purposes. Genetic data is regarded to be unique and very sensitive as it has the potential of revealing in the future personal, scientific and medical information of each patient including the family members of the data subject.[129] For this reason, genetic research projects typically handle anonymized data using advanced encryption tools in order to safeguard patients' privacy rights and be in compliance with data protection laws. Once the data has become entirely anonymous, it is ready to be used by the research community. It is not the purpose of this chapter to discuss data protection matters; rather this section focuses on answering the question: who has the "ownership" rights of such data and databases? Or, who is allowed to *use* and get *access* to such data for scientific research purposes? In other words, it is more about the controllability of data and databases. And, to point to some general features of the SLA that, in tandem with the risk assessment tool, may help to clarify and mitigate some of the uncertainties around these questions.

For this reason, the role of the broker in this type of use case scenario is very important as it can take a fiduciary nature as a trusted third party and audit such compliance. The broker can intervene and be in charge of engaging with end-users (in this case the hospitals or research institutions) and the Cloud providers. At the same time, some of the brokers may correct the complaints or requests of the end-users and serve as a gate away to information necessary to clarify and rectify the contractual terms of the SLA. This provides the opportunity to expand its assistance as a mere agent considerably beyond the model for what has already been established and cover various use case scenarios within an international framework. Figures 5 and 6 illustrate some of the risk assessment features that fall within the "policy" and "legal" categories as follows:

Finally, when the researchers and doctors use a Cloud computing service to store and process the data of patients, they are particularly concerned about the confidentiality and integrity of such data. These two aspects are integral parts of the

[129]Article 29 Data Protection Working Party (2004), pp. 1–14.

Fig. 5 Example of policy/legal category

- Risk Category: **Policy/Legal**.
- Asset Identified: Data ("ownership" rights of new data generated by Big Data applications).
- Vulnerability of Asset: Lack of clarification within the SLA of who is allowed to use and access the new data generated in the Cloud.
- Threat to Asset: SLA.
- Risk Likelihood: Possible.
- Risk Impact: Extreme.
- Resulting Risk Level: Product of risk likelihood and risk impact = High.
- Risk Event: Negligence: This risk takes place at steps number 1 and 3 (see Figure 4 above). That is, when the broker sends the SLA request to various Cloud providers and then filters the offers received. In this case the broker must choose the provider according to end-user's criteria.
- Resulting Risk Mitigation: Include a *string* field capability within the SLA, which allows the inclusion of contractual clauses that can clarify who is allowed to use and access this data e.g., for scientific research.

security infrastructure, but also, in particular, the *availability* of such data during a time of crisis. While confidentiality refers to the property of data or information not being made available or disclosed to unauthorized persons,[130] integrity means that the information must be accurate, not allowing data to be modified.[131] Availability, on the other hand, is concerned with ensuring that data and services are accessible where and when it is needed with the proviso that is consistent with the SLA legal framework.[132]

In the event of any disaster (e.g., earthquake, floods, etc.), the risk assessment framework through the CBS may help to fix the situation immediately and fill the gap in emergency situations. According to the ISO 27001, availability is: "a characteristic that applies to assets. An asset is available if it is accessible and usable when needed by an authorized entity. In the context of this standard, assets include things like information, systems, facilities, networks, and computers."[133] From a

[130]Gough and Nettleton (2010), p. 149.

[131]Kattan et al. (2011), p. 199.

[132]Williams (2013), p. 187; Bonewell (2006), p. 1178.

[133]For this term see, e.g., http://www.praxiom.com/iso-27001-definitions.htm. Accessed 10 October 2016.

Fig. 6 Example of legal category

- Risk Category: **Legal**.
- Asset Identified: Databases.
- Vulnerability of Asset: Database rights may create some constraints for scientific research.
- Threat to Asset: Database rights.
- Risk Likelihood: Possible.
- Risk Impact: Major.
- Resulting Risk Level: High.
- Risk Event: Negligence: This risk takes place at steps number 1 and 3 (see Figure 4 above). That is, when the broker sends the SLA request to various Cloud providers and then filters the offers received. In this case the broker must choose the provider according to end-user's criteria.
- Resulting Risk Mitigation: Clearly define database rights within the SLA through the XML Description Schema and add a Boolean "waiving" system whereby the Cloud provider can choose to *keep* or *waive* database rights based on end-user's input.

Fig. 7 Example of technical/general category

- Risk Category: **Technical/General**.
- Asset Identified: Availability of Data and Databases.
- Vulnerability of Asset: Lack of maintenance.
- Threat to Asset: Database server failure.
- Risk Likelihood: Rare.
- Risk Impact: Moderate.
- Resulting Risk Level: Product of risk likelihood and risk impact = Low.
- Risk Event: Unavailability of data due to server failure: This risk takes place at step number 5 (see Figure 4 above) during service operation. That is, when the Cloud provider is running the service and unexpectedly there is a server failure e.g., one or more VMs stop running.
- Resulting Risk Mitigation: Fault-tolerance solutions provision.

Fig. 8 Example of technical/general category

- Risk Category: **Technical/General**
- Asset Identified: Availability of data and databases.
- Vulnerability of Asset: Data center infrastructure (servers).
- Threat to Asset: Force majeure (such as floods, earthquakes, etc.).
- Risk Likelihood: Rare.
- Risk Impact: Major.
- Resulting Risk Level: Product of risk likelihood and risk impact = Medium.
- Risk Event: Unavailability of data due to server failure: This risk takes place at step number 5 (see Figure 4 above) during service operation. That is, when the Cloud provider is running the service and unexpectedly there is an event of force majeure.
- Resulting Risk Mitigation: Redundancy and use of back-up servers located in different places (cities): Data should be constantly replicated with databases and back-up solutions during the whole Cloud computing service life cycle.

legal perspective, "availability" is strongly related to "ownership" rights of data as this also refers to the legal wherewithal to control and make good use of data.

The threat analysis suggests that the risk ratings belonging to availability are classified as *medium* in comparison to confidentiality (high) and integrity (low). This is because the end-users (or patients in this case) are more concerned with their privacy. Therefore, confidentiality has a stronger effect on trust and the provider's reputation. Integrity can be caused by accidental software and user errors, equipment failure and deliberate alteration of data by third parties. It is relatively low because the impact is much lower in comparison to the availability of data. Loss of availability is classified as medium since end-users and enterprises are better off using Cloud computing provider resources rather than deploying their own infrastructure taking into account the cost benefits (Figs. 7 and 8).[134]

[134]Kahn et al. (2012), p. 124.

10 Conclusion

As with any intellectual property matter, the European Database Directive was designed to counterbalance two opposite forces. Along the same lines, it is true that database protection is an instrument that may foster innovation and investment within the database industry. On the opposing end, stringent laws such as database rights may also create potential conflicts with regulations that are not compatible,[135] especially if we consider the global and ubiquitous nature of the Cloud. In addition, the Big Data movement raises the question of "ownership" rights in the new data generated. This issue is far from being clear as this concept glosses over many aspects that ought to be clearly specified during SLA negotiation.

Increasing interest in the use of SLAs to govern interactions in Cloud computing transactions has gained momentum. While such agreements are a vital component to ensure a successful relationship between end-users and Cloud providers, they are limited in scope and coverage. Such limitations may give rise to considerable exposure of risks not only for end-users, but also for service providers. Therefore, a risk assessment component has been fully implemented in the OPTIMIS software toolkit, which aligns with the SLA framework in the context of Grid and Cloud resource brokers. This model provides a solution as to how to express these requirements on a technical level in the SLAs and the data management system. It has also been equipped with a monitoring tool as well as the requirements of an inherent legal risk inventory, which provides an additional layer of legal protection. This enables very fine-grained and continuous control over the data and databases. Thus, allowing the identification of the sort of actions that are needed to reduce and mitigate such risks. Crucially, this new framework attempts, not only to raise collective awareness of the risks entailed in a neglected area of research, but also at increasing confidence levels, prompting the involved parties to trust each other to a greater extent than is currently the case.

Acknowledgements This work has been partially supported by the EU within the 7th Framework Program under contract ICT-257115—Optimized Infrastructure Services (OPTIMIS), and, by the Japanese Ministry of Education, Culture, Sports, Science, and Technology (MEXT) through a research scholarship (Mombukagakusho) conducted at Kyushu University in Japan. The authors would like to thank Prof. Toshiyuki Kono, Prof. Shinto Teramoto and Rodrigo Afara for their valuable guidance.

References

Advanced Risk Assessment and Management for Trustable Grids (AssessGrid). EU funded project within the FP6 IST Framework Program under contract no. 031772 http://cordis.europa.eu/project/rcn/79340_en.html

[135]Maurer et al. (2001), p. 789; Maurer (2008), pp. 13-4–13-80.

Andrieux A et al (2007) Web services agreement specification (WS-agreement). Global Forum
American Heritage Dictionary. https://www.ahdictionary.com/word/search.html?q=risk&submit.x=-872&submit.y=-210. Accessed 15 Oct 2016
Art. 29 Data Protection Working Party (2004) Working document on genetic data adopted on 17 March 2004. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2004/wp91_en.pdf. Accessed 10 Oct 2016
Batré et al (2007) Gaining users' trust by publishing failure probabilities. In: Security and privacy in communications networks and the workshops, 2007. SecureComm 2007. Proceedings of the third international conference on security and privacy in communication networks, Nice
Beckers K (2015) Pattern and security requirements: engineering-based establishment of security standards. Springer, Cham
Bently L, Sherman B (2009) Intellectual property law, 3rd edn. Oxford University Press, Oxford
Bonewell D (2006) Security and privacy for data warehouses: opportunity or threat? In: Tipton H, Krause M (eds) Information security management handbook, 5th edn. Auerbach Publications, Boca Ratón
Bradshaw S, Millard C, Walden I (2010) Contracts for clouds: comparison and analysis of the terms and conditions of cloud computing services. Queen Mary School of Law Legal Studies research paper no. 63/2010. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1662374. Accessed 10 Oct 2016
Burnett R (2005) Legal risk management for the IT industry. Comput Law Secur Rep 21(1):61–67
Cawsey A. Rule-based systems. http://www.zemris.fer.hr/predmeti/krep/Rules.pdf. Accessed 10 Oct 2016
Cattedu D, Hogben G (2009) Cloud computing: benefits, risks and recommendations for information security. ENISA (European Network and Information Security Agency). http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport. Accessed 10 Oct 2016
Cayirci E (2015) Models for cloud risk assessment: a tutorial. In: Felici M, Fernández-Gago C (eds) Accountability and security in the cloud: first summer school, cloud accountability project, A4cloud, Malaga, Spain, June 2–6 2014, revised selected papers and lectures. Springer, Cham
Chander A (2013) The electronic silk road: how the web binds the world together in commerce. Yale University Press, New Haven
Chung L et al (2000) Non-functional requirements in software engineering. Springer, New York
Chung L, Sampaio Do Prado Leite J (2009) On non-functional requirements in software engineering. In: Borgida A et al (eds) Conceptual modeling: foundations and applications: essays in honor of John Mylopoulos (Lecture notes in computer science/Information systems and applications, incl. internet/web, and HCI, vol 5600). Springer, Berlin
Ciborra C (2005) Digital technologies and the duality of risk. Centre for Analysis of Risk and Regulation. London School of Economics and Political Science, London
Ciborra C (2007) Digital technologies and risk: a critical review. In: Hanseth O, Ciborra C (eds) Risk, complexity and ICT. Edgar Elgar Publishing, Cheltenham
Ciborra C (2009) Imbrication of representations: risks and digital technologies. In: Avgerou C, Lanzara F, Willcocks L (eds) Bricolage, care and information systems: Claudio Ciborra's legacy in information systems research. Palgrave MacMillan, New York
Corrales M (2012) Privacy risk impact assessment: a new requirement for safer clouds. Beck-Online, ZD-Aktuell, 03036
Davison M (2003) The legal protection of databases. Cambridge University Press, Cambridge
Dean J (2014) Big data, data mining and machine learning: value creation for business leaders and practitioners. Wiley, Hoboken
DG Internal Market and Services Working Paper, First Evaluation of Directive 96/9/EC on the Legal Protection of Databases. http://ec.europa.eu/internal_market/copyright/docs/databases/evaluation_report_en.pdf. Accessed 10 Oct 2016
Disselkamp L (2013) Workforce asset management book of knowledge: official guide for workforce asset management certification. Wiley, Hoboken

Djemame K et al (2011a) A risk assessment framework and software toolkit for cloud service ecosystems. In: The second international conference on cloud computing, GRIDs, and virtualization. http://www.optimis-project.eu/content/risk-assessment-framework-and-software-toolkit-cloud-service-ecosystems. Accessed 10 Oct 2016

Djemame K et al (2011b) Brokering of risk-aware service level agreements in grids. Concurr Comput Pract Exp 23:1558–1582

Djemame K et al (2012) Legal issues in the cloud: towards a risk inventory. Philos Trans R Soc A 371(1983):20120075

Djemame K et al (2016) A risk assessment framework for cloud computing. IEEE Trans Cloud Comput 4(3):265–278

Draft White Paper on Legal Options for the Exchange of Data through the GEOSS Data-CORE. Group on Earth Observations. https://www.earthobservations.org/documents/dsp/draft_white_paper_geoss_legal_interoperability_30_october_2011.pdf. Accessed 10 Oct 2016

Drissi S, Houmani H, Medromi H (2013) Survey: risk assessment for cloud computing. Int J Adv Comput Sci Appl 4(12):143–148

Dupré L, Haeberlen T (eds) (2012) Cloud computing: benefits, risks and recommendations for information security. ENISA European Network and Information Security Agency. https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security. Accessed 10 Oct 2016

Fellows W (2013) Cloud brokers: now seeking ready-to-pay customers, 451 research. https://451research.com/report-long?icid=2666. Accessed 10 Oct 2016

Fellows W, Ring, K, Rogers O (2014) Cloud brokers: making ITAAS a practical reality? https://451research.com/images/Marketing/DIS/451_CloudBrokers_2014_FINAL.pdf. Accessed 10 Oct 2016

Ferrer et al (2011) OPTIMIS: a holistic approach to cloud service provisioning. Future Gener Comput Syst 28:66–77

GEOSS-Data Core Project. https://www.earthobservations.org/documents/dswg/Annex%20VI%20-%20%20Mechanisms%20to%20share%20data%20as%20part%20of%20GEOSS%20Data_CORE.pdf. Accessed 10 Oct 2016

Garner B (ed) (2014) Black's law dictionary, 10th edn. Thomson Reuters, St. Paul

Gough J, Nettleton D (2010) Managing the documentation maze: answers to questions you didn't even know. Wiley, Hoboken

Gourlay I, Djemame K, Padgett J (2008) Reliability and risk in grid resource brokering. In: 2008 second IEEE international conference on digital ecosystems and technologies (IEEE DEST 2008)

Gourlay I, Djemame K, Padgett J (2009) Evaluating provider reliability in grid resource brokering. In: 11th IEEE international conference on high performance computing and communications

Grosan C, Abraham A (2011) Ruled-based expert systems. In: Grosan C, Abraham A (eds) Intelligent systems: a modern approach, intelligent systems reference library, vol 17. Springer, Berlin

Großmann J, Seehusen F (2016) Combining security risk assessment and security testing based on standards. In: Seehusen et al (eds) Risk assessment and risk-driven testing: third international workshop, RISK 2015, Berlin, Germany. Springer, Cham

Gutwirth S, Hildebrandt M (2010) Some caveats on profiling. In: Gutwirth S, Poullet Y, de Hert P (eds) Data protection in a profiled world. Springer, Dordrecht

Holzinger A et al (2013) Combining HCI, natural language processing, and knowledge discovery—potential of IBM content analytics as an assistive technology in the biomedical field. In: Holzinger A, Pasi G (eds) Human computer interaction and knowledge discovery in complex, unstructured, big data, third international workshop, HCI-KDD 2013, Maribor, Slovenia, July 2013, Proceedings. Springer, Heidelberg

Ishikawa H (2015) Social big data mining. CRC Press, Boca Ratón

ISO 22307:2008 Financial services—privacy impact assessment. http://www.iso.org/iso/catalogue_detail.htm?csnumber=40897. Accessed 10 Oct 2016

ISO 31000:2009 Risk management. https://www.iso.org/obp/ui/#iso:std:43170:en. Accessed 10 Oct 2016

ISO/IEC 29101:2013. Information technology—Security techniques—privacy architecture framework. http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=45124&commid=45306. Accessed 10 Oct 2016

ISO/IEC DIS 29134 Information technology—Security techniques—privacy impact assessment—guidelines. http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=62289. Accessed 10 Oct 2016

ISO/IEC NP 19086-4 Information technology—cloud computing—service level agreement (SLA) framework and technology—part 4: security and privacy. http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=68242. Accessed 10 Oct 2016

Jackson P (1998) Introduction to expert systems, 3rd edn. Addison-Wesley, Harlow

Jones B, Bird I (2013) Data-intensive production grids. In: Critchlow T, Kleese van Dam K (eds) Data-intensive science. Chapman & Hall (CRC Press), Boca Ratón

Kasemsap K, Sunandha S (2015) The role of cloud computing adoption in global business. In: Chang V, Walter R, Wills G (eds) Delivery and adoption of cloud computing services in contemporary organizations. Information Science Reference (IGI Global), Hershey

Kattan I, Nunu A, Saleh K (2011) A stochastic model for improving information security in supply chain systems. In: Wang J (ed) Supply chain optimization, management and integration: emerging applications. Business Science Reference, Hershey

Khan A et al (2012) Security risks and their management in cloud computing. In: 2012 IEEE 4th international conference on cloud computing technology and science, IEEE Computer Society

Kingston W (2010) Beyond Intellectual Property: Matching Information Protection to Innovation. Edward Elgar Publishing, Cheltenham

Kirkham T et al (2012) Assuring data privacy in cloud transformations. In: 2012 IEEE 11th international conference on trust, security and privacy in computing and communications

Kirkham T et al (2013) Richer requirements for better clouds. In: 2013 IEEE International conference on cloud computing technology and science. IEEE Computer Society

Kitchin R (2014) The data revolution: big data, open data, data infrastructures & their consequences. Sage Publications, Los Angeles

Kousiouris G, Vafiadis G, Corrales M (2013) A cloud provider description schema for meeting legal requirements in cloud federation scenarios. In: Douligeris et al (eds) Collaborative, trusted and privacy-aware e/m-services, 12th IFIP WG 6.11 conference on e-business, e-services, and e-society, I3E 2013, Athens, Greece, 25–26 Apr 2013, Proceedings. Springer, Heidelberg

Krishnan K (2013) Data warehousing in the age of big data. Elsevier, Amsterdam

Lebber D, Hermann J (2013) Decision analysis methods for selecting consumer services with attribute value uncertainty. In: Lee ML et al (eds) Risk assessment and evaluation of predictions. Springer, New York

Legal risk management. http://www.jus.uio.no/ifp/english/about/organization/nrccl/research-areas/ongoing-research/legal-risk-management.html#ref1. Accessed 10 Oct 2016

Li T, Singh M (2014) Hybrid trust framework for loss of control in cloud management. In: Jeong H et al (eds) Advances in computer science and its applications: CSA 2013. Springer, Heidelberg

Lohr S (2015) Data-ism: the revolution transforming decision making, consumer behavior, and almost everything else. HarperCollins Publishers, New York

Luiijf E (2016) Threats in industrial control systems. In: Colbert E, Kott A (eds) Cyber-security of SCADA and other industrial control systems. Springer, Cham

Lund M, Solhaug B, Stolen K (2011) Model-driven risk analysis: the CORAS approach. Springer, Heidelberg

Mahmood Z (ed) (2014) Continued rise of the cloud: advances and trends in cloud computing. Springer, London

Majkic Z (2014) Big data integration theory: theory and methods of database mappings, programming languages, and semantics. Springer, Cham

Maurer S (2008) Across two worlds: database protection in the United States and Europe. In: Putnam J (ed) Intellectual property and innovation in the knowledge-based economy, conference proceedings, 23–24 May 2001, Toronto, Canada. University of Calgary Press, Calgary

Maurer S, Hugenholtz B, Onsrud H (2001) Europe's database experiment. Science 294:789–790

Nwankwo S (2014) Developing a risk assessment methodology for data protection. IRI Blog. https://blog.iri.uni-hannover.de/index.php/2014/12/17/developing-a-risk-assessment-methodology-for-data-protection/. Accessed 10 Oct 2016

OECD principles and guidelines for access to research data from public funding, OECD 2007. http://www.oecd.org/sti/sci-tech/38500813.pdf. Accessed 10 Oct 2016

Optimized Infrastructure Services (OPTIMIS). EU funded project within the 7th Framework Program under contract ICT-257115. http://www.optimis-project.eu. Accessed 10 Oct 2016

Padgett J et al (2009) Risk-aware SLA brokering using WS-agreement. In: Awan I et al (eds) Conference proceedings: 23rd international conference on advanced information networking and applications, AINA 2009, IEEE Computer Society, proceedings. The Institute of Electrical and Electronics Engineers Inc., Danvers

Peng G, Dutta A, Choudhary A (2014) Exploring critical risks associated with enterprise cloud computing. In: Leung V, Chen M (eds) Cloud computing: 4th international conference, CloudComp 2013, Wuhan, China. Springer, Cham

Plain English ISO 31000:2009. Risk management dictionary. http://www.praxiom.com/iso-31000-terms.htm. Accessed 10 Oct 2016

Rejas-Muslera R, Cuadrado-Gallego J, Rodriguez D (2007) Defining a legal risk management strategy: process, legal risk and lifecycle. In: Abrahamsson P et al (eds) Software process improvement. Lecture notes in computer science, programming and software engineering, proceeding of the 14th European software process improvement conference, EuroSPI 2007, Potsdam, Germany, Sept 2007. Springer, Berlin

Ridley E (2015) Big Data and Risk Assessment. In: Kalyvas J, Overly M (eds) Big data: a business and legal guide. CRC Press, Boca Ratón

Sakr S, Gaber M (eds) (2014) Large scale and big data: processing and management. CRC Press, Boca Ratón

Sangrasi A, Djemame K, Johkio I (2012) Aggregating node level risk assessment in grids using an R-out-of-N model. In: Bhawani S et al (eds) (2012) Emerging trends and applications in information communication technologies: second international multi topic conference, IMTIC 2012, Jamshoro, Pakistan, March 2012, proceedings, communications in computer and information science, vol 281. Springer, Heidelberg

Shantz J (2005) Beyond risk and boredom: reflexions on Claudio Ciborra and sociology. Eur J Inf Syst 14:510–512

Sharif A, Basri S (2011) Software risk assessment: a review on small and medium software projects. In: Zain J et al (eds) Software engineering and computer systems, second international conference ICSECS 2011, Kuantan, Pahang, Malaysia, June 2011, proceedings part 2. Springer, Heidelberg

Summary White Paper, Legal options for the exchange of data through the GEOSS Data CORE. Data Sharing Task Force, Group on Earth Observations

Summer J, Ross T, Ababouch L (2004) Application of risk assessment in the fish industry. FAO Fiesheries technical paper no 442, part 1

Sundara Rajan M (2011) Moral rights: principles, practice and new technology. Oxford University Press, Oxford

Susskind R (1998) The future of law. Oxford University Press, Oxford

Taubenberger S et al (2011) Problem analysis of traditional IT-security risk assessment methods—an experience report from the insurance and auditing domain. In: Camensich J et al (eds) Future challenges in security and privacy for academia and industry: 26th IFIP TC 11 international information security conference, SEC 2011, Lucerne, Switzerland, June 2011, proceedings. Springer, Heidelberg

Teng F, Magoules F (2010) Future of grids resources management. In: Magoules F (ed) Fundamentals of grid computing: theory, algorithms and technologies. Chapman and Hall/CRC Press, Boca Ratón

Toosizadeh S, Reza Farshchi S (2011) Ruled-based programming for building expert systems: how do you create an expert system? Lambert Academic Publishing, Saarbrücken

Vashist R (2015) Cloud computing infrastructure for massive data: a gigantic task ahead. In: Hassanien A et al (eds) Big data in complex systems: challenges and opportunities, studies in big data, vol 9. Springer, Cham

Vaquero L et al. (2008) A break in the clouds. ACM SIGCOMM Comput Commun Rev 39(1):50

Vraalsen F et al. (2005) Specifying legal risk scenarios using the CORAS threat modeling language: experiences and the way forward. In: Herrmann P, Issarny V, Shiu S (eds) Trust management, third international conference, iTrust 2005, Paris, France, 23–26 May 2005. Proceedings, vol 3477. Springer, Berlin

Wahlgren P (2007) Legislative Techniques. In: Wintgens L (ed) Legislation in context: essays in legisprudence, applied legal philosophy. Ashgate Pub Co., Hampshire

White Paper, Mechanisms to share data as part of GEOSS Data-CORE. https://www.earthobservations.org/documents/dswg/Annex%20VI%20-%20%20Mechanisms%20to%20share%20data%20as%20part%20of%20GEOSS%20Data_CORE.pdf. Accessed 10 Oct 2016

Williams P (2013) Information security governance: a risk assessment approach to health information systems protection. In: Hovenga E, Grain H (eds) Health information governanc in a digital environment. IOS Press, Amsterdam

Wintgens L, Thion P (2007) Introduction. In: Wintgens L (ed) Legislation in context: essays in legisprudence, applied legal philosophy. Ashgate Pub Co., Hampshire

Wright D, De Hert P (eds) (2012) Privacy impact assessment, law, governance and technology series, vol 6. Springer, Dordrecht

Wu L et al (2013) Automated SLA negotiation framework for cloud computing. In: International symposium on cluster, cloud and grid computing (CCGrid), 2013 13th IEEE/ACM, May 13016, Delft, The Netherlands. https://pdfs.semanticscholar.org/6660/3838e3d4e2bdec718bed6b94d8cd730aea26.pdf?_ga=1.212388371.624674434.1462343094. Accessed 10 Oct 2016

XML Description Schema. http://www.optimis-project.eu/content/xml-description-schema-improvement. Accessed 10 Oct 2016

Internet Intermediaries and Copyright Enforcement in the EU: In Search of a Balanced Approach

Ioannis Revolidis

Abstract Ever since the commercialization of the Internet, the role of Internet intermediaries has been of vital importance for the functioning of the globalized electronic market and the innovation technologies of information dissemination in general. The importance of the role of the Internet intermediaries has been reflected in the basic legislative initiatives regarding the Internet worldwide. In Europe, following the example of the Communications Decency Act (CDA) and Digital Millennium Copyright Act (DMCA) in the United States, Articles 12–15 of the E-Commerce Directive aimed to create an immunity regime that would allow the Internet intermediaries to develop their activities without being hindered by the fear of complex liability issues connected with their sensitive role. At the same time, though, it became apparent that Internet intermediaries are playing a pivotal role in the protection of intellectual property rights in an online world, as they are in the best position to either prevent or bring intellectual property infringements to an end. This observation was also reflected in the EU legislation, as Articles 12, 13 and 14 of the E-Commerce Directive, Article 8 of the InfoSoc Directive and Article 9 and 11 of the Enforcement Directive provide for a series of interim measures that allow legal action against Internet intermediaries for alleged copyright infringements by third parties (even if the Internet intermediaries are not liable per se). This chapter will first try to highlight what are the current patterns dictated by the case law of the Court of Justice of the European Union (CJEU) regarding the role of Internet intermediaries in the enforcement of intellectual property rights and then attempt to assess whether these patterns correspond to the legislative motives and purposes behind the respective EU legislation.

Keywords E-Commerce · EU fundamental rights · Internet intermediaries · Copyright enforcement online · Injunctions against internet intermediaries

I. Revolidis (✉)
Institute for Legal Informatics, Leibniz Universität Hannover, Hannover, Germany
e-mail: ioannis.revolidis@iri.uni-hannover.de

M. Corrales et al. (eds.), *New Technology, Big Data and the Law*,
Perspectives in Law, Business and Innovation, DOI 10.1007/978-981-10-5038-1_9

Contents

1 Introduction

The activities of Internet intermediaries constitute the basic backbone of current Internet technology and their functioning has therefore obtained paramount significance in the process of distributing information online. All the essential check points along the way of a distribution channel, starting from the initiation of the information dissemination process all the way up to its final destination, are under their supervision and control.

Their position has nonetheless become rather unpleasant; taking into account that such significance comes not only with important benefits, but also with a considerable price. The price that the Internet intermediaries have to pay is that they must compromise, settle and satisfy the usually diverse, contradicting and conflicting interests that revolve around the Internet economy. It is thus not surprising that their special role has, from relatively early, been the focus of Internet related case law,[1] Internet legislation debates[2] and academic discussion on Internet regulation.[3]

[1]The US courts had to adjudicate on the rules applicable to Internet intermediaries as early as the beginning of the 1990s, in cases such as Cubby v Compuserve 766 F Supp 135 (SDNY, 1991) and Stratton Oakmont, Inc. v Prodigy Services 1995 WL 323710 (N.Y. Sup. Ct., 1995).

[2]Internet intermediaries were in fact in favor of legislative initiatives regarding their role in Internet regulation already during the early days of the commercial use of the Internet, pleading for an immunity regime that would allow them to operate without unnecessary or disproportionate legal risks. See to that extend, Edwards (2005), p. 102.

[3]Most characteristically, Lessig (2006), pp. 81–137. For a similar account, see Goldsmith and Wu (2008), pp. 65–85.

Taking into account that the Internet has revolutionized the way of distributing information,[4] it is not surprising that copyright related issues have usually been high in the agenda of Internet intermediary regulation. The traditional copyright industry has looked upon Internet intermediaries not only as potential litigation targets, but also as private enforcement agents that shall overtake the role of imposing copyright rules online.[5] Assigning such a role to Internet intermediaries has severe consequences on the character and future of the whole medium, as it drastically affects the quantity and quality of information that flows within the different distribution channels. A strong involvement of Internet intermediaries in the field of online copyright enforcement will put the neutral character of the medium at stake and, with it, all the industry and user rights that are depending on that neutral character.[6] Additionally, a strict copyright enforcement regime delivered via the Internet intermediaries might severely damage the potential for innovation and economic growth within a digital market.

It is this sensitive role of Internet intermediaries and the complexity of the legal issues attached to it that prompted many legislators across the world to come up with special regimes regarding their role and responsibilities.[7] National responses to intermediary liability vary.[8] What seems to be the prevalent model is the creation of

[4]Mostly by offering a wider range of discretion on the production, selection and dissemination of information in comparison to other traditional media, turning thus the users from simple passive receivers to interactive stakeholders. See Wu (2011), pp. 168–203. For an insightful assessment of the particularities of the Internet, see Svantesson (2016), pp. 56–78, who emphasizes the importance of Internet intermediaries by noting (p. 74): "…The fact that intermediaries play a central role in the Internet landscape is little more than a truism and has already been allude to above. However, the role they play is of such central importance that we may indeed conclude that they are as important a feature of the Internet, and Internet regulation, as any other of the characteristics discussed here. After all, we all connect to the Internet via intermediaries (such as the telecommunications companies we contract with), and most of our online activities go via intermediaries (such as Google or Bing search, shopping platforms such as eBay and social media platforms such as Facebook)…".

[5]For the role of Internet intermediaries as private copyright enforcers, see Zittrain (2003), pp. 653–688; Frabboni (2010), pp. 119–146; Bright and Agustina (2013), pp. 120–137.

[6]In the words of Marsden (2011), pp. 53–64, the neutral character of the Internet shall be protected by regulations that: "… prevent unregulated non-transparent controls exerted over traffic via DPI equipment, whether imposed by ISPs for financial advantage or by governments eager to use this new technology to filter, censor and enforce copyright against their citizens …".

[7]The two primary provisions of US law, namely section 230 of the "Communications Decency Act" (CDA) and section 512 of the "Digital Millennium Copyright Act" (DMCA), are usually recorded as archetypes of such legislative initiatives, not only because they represent some of the earliest regulations of the kind, but also because many major Internet companies are established in the USA, offering thus the conditions for debates of that kind. For a similar account see Holland et al. (2015), p. 1.

[8]For a classification of legislative responses to intermediary liability, see Edwards (2005), pp. 106–113. For a taxonomy of the legislative responses to intermediary liability and their economic effectiveness, see Schruers (2002), pp. 205–264.

a conditional immunity regime for Internet intermediaries, where they can avoid any primary liability, if they fulfill certain criteria (most commonly if they display a "passive" role in the process of disseminating information online).[9]

The European legislator has acknowledged the potential risks surrounding the role of Internet intermediaries and their possible negative impact on the creation of a common European electronic market relatively early.[10] The decision was taken, therefore, to create a unified immunity regime for certain types of Internet intermediaries in Articles 12–15 of the E-Commerce Directive.[11] Internet service providers that can be classified as mere conduits,[12] caching operators[13] or hosting providers[14] are exempted from direct legal action against them, provided that they fulfill the conditions prescribed in the E-Commerce Directive.

That conditional immunity of Internet service providers does not mean that they are relieved from every duty that revolves around their key role as gatekeepers of the online communications. The E-Commerce Directive aimed to be "the appropriate basis for the development of rapid and reliable procedures for removing and disabling access to illegal information,"[15] albeit, without providing for a unified intermediary code of conduct or a unified "notice and take down" system.[16] The creation of such institutions was entrusted to the national legislators of the Member States, leading to a considerable level of legal uncertainty within the common European market.[17] This uncertainty stems from the (reasonably expected) variations that have been monitored in the development of such national codes of intermediary conduct or "notice and take down" systems.[18]

---

[9]Reed (2003), pp. 255–265, seems to propose that such a conditional immunity regime could be the basis of a unified global solution in terms of Internet intermediary regulation.

[10]Recital 40 of the E-Commerce Directive: "Both existing and emerging disparities in Member States' legislation and case-law concerning liability of service providers acting as intermediaries prevent the smooth functioning of the internal market, in particular by impairing the development of cross-border services and producing distortions of competition…".

[11]Directive 2000/31/EC of the European Parliament and the Council.

[12]Article 12, E-Commerce Directive.

[13]Article 13, E-Commerce Directive.

[14]Article 14, E-Commerce Directive.

[15]As stated in recital 40.

[16]On the contrary Sections 512 (c) and (g) of the American DMCA provide for such a system. For a closer scrutiny of the DMCA "notice and take down" system, see Cobia (2009), pp. 387–411.

[17]Early commentators have criticized the lack of a European intermediary code of conduct and "notice and take down system" on such a basis. See, e.g., Juliá-Barceló and Koelman (2000), pp. 231–237; Baistrocchi (2002), pp. 111–130.

[18]For a neat summary of the basic "notice and take down" issues that would have preferably been unified within the EU, see Edwards and Waelde (2005), pp. 28–36.

The lack of a coordinated and effective European "notice and take down" procedure[19] has shifted the interest of the involved stakeholders to other potential enforcement remedies. Court injunctions against Internet intermediaries, especially in the field of copyright enforcement, have thus become rather popular. Such judicial remedies are facilitated not only in Article 12 (3), 13 (2) and 14 (3) of the E-Commerce Directive but also in Article 8 (3) of the InfoSoc Directive[20] and Articles 9 (1) (a) and 11 of the Enforcement Directive.[21] The attractiveness of such a remedy lies on the fact that it can be ordered against intermediaries irrespective of any liability, namely even if the affected information society service provider would otherwise be granted the immunities of the E-Commerce Directive.[22] The reason behind this legal peculiarity of allowing court action against an otherwise non-liable party is founded on the key position of Internet intermediaries within an information distribution network. By being the natural gatekeepers of the information exchange, they can easily prevent or terminate any illegal activities.[23]

Although EU law obliges the Member States to make such remedies against intermediaries available to right holders, it does not prescribe the procedural modalities and guarantees that shall govern them. That is a task left to the legislators and judges of the Member States,[24] although the CJEU is offering its authoritative guidance. Even so, the fact that such remedies will be issued in the form of a judicial decision, benefiting thus from all the corresponding enforcement privileges of civil procedural law, has made them very much attractive for the copyright holders who are applying for them rather often. This chapter will focus on the scope of such injunctions, as the case law of the CJEU on that area has kindled a vivid discussion in the EU.

[19]On the low effectiveness of Member State "notice and take down systems" and a comparative analysis with their international counterparts, see Giblin (2014), pp. 147–210.

[20]Directive 2001/29/EC of the European Parliament and the Council.

[21]Directive 2004/48/EC of the European Parliament and the Council.

[22]As it is explained in Recital 45 of the E-Commerce Directive: "The limitations of the liability of intermediary service providers established in this Directive do not affect the possibility of injunctions of different kind…".

[23]Recital 59 of the InfoSoc Directive provides that: "In the digital environment, in particular, the services of intermediaries may increasingly be used by third parties for infringing activities. In many cases, such intermediaries are best placed to bring such infringing activities to an end. Therefore, without, prejudice to any other sanctions and remedies available, right holders should have the possibility of applying for an injunction against an intermediary who carries a third party's infringement of a protected work or other subject-matter in a network."

[24]See Recital 59 of the InfoSoc Directive ("…The conditions and modalities relating to such injunctions should be left to the national law of the Member States.") and the almost identical Recital 23 of the Enforcement Directive ("…The conditions and procedures relating to such injunctions should be left to the national law of the Member States …").

2 Dramatis Personae: The Ratione Personae Scope of Injunctions Against Internet Intermediaries in EU Copyright Law

2.1 General Overview

As noted above, injunctions are addressed to Internet intermediaries. The outer limits of that legal category are to be traced in the E-Commerce Directive. Internet intermediaries are information society service providers within the meaning of Article 2 (b) of the E-Commerce Directive, namely any natural or legal person that offers services "…normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services…"[25] At first glance, such a wide definition seems to open up an endless circle of possible recipients of an injunction mandate, as the majority of Internet operators falls within the aforementioned definition.

Such a broad approach seems to be further supported by Article 8 (3) of the InfoSoc Directive. As it has been highlighted in legal doctrine,[26] the CJEU seems to identify an "intermediary" within the premises of Article 8 (3) of the InfoSoc Directive, as any Internet operator who provides a service capable of being used by a third party to infringe,[27] using the ability of an online service provider to put an end to a copyright infringement as the sole limitation of the examined notion.[28]

The exact depth of the legal category "Internet intermediary" shall nonetheless be specified further within the premises of the E-Commerce Directive. Firstly, because by virtue of its scope[29] the E-Commerce Directive seems to take precedence in regulating the conditions and modalities that refer to the development of the common European digital market (including, inter alia, the premises under which the Internet intermediaries shall operate). Secondly, although both the InfoSoc and the Enforcement Directives have an undisputed impact on the regulation of certain aspects of the common digital copyright market, neither of them shall affect the provisions of the E-Commerce Directive, as it is confirmed from a

[25]See Article 1 (2) of Directive 98/34/EC as amended by Directive 98/48/EC. For a closer inspection of the individual elements of the definition, see Riordan (2016), Chapter 12, Section 2.

[26]Husovec & Peguera (2015), p. 13.

[27]Such an assumption could be founded on par. 43 in case C-557/07, LSG v. Tele2, where the Court noted: "Access providers who merely enable clients to access the Internet, even without offering other services which users make use of, provide a service capable of being used by a third party to infringe a copyright or related right, inasmuch as those access providers supply the user with the connection enabling him to infringe such rights."

[28]Husovec & Peguera (2015), pp. 13 in fine.

[29]See Article 1, E-Commerce Directive.

parallel reading of Recital 16 of the InfoSoc Directive[30] and Article 2 (3) (a) of the Enforcement Directive[31] and also seems to be further supported by the case law of the CJEU.[32]

2.2 *Internet Intermediaries According to the E-Commerce Directive*

It is thus within the premises of the E-Commerce Directive that the exact depth of the legal category "Internet intermediaries" shall be explored. As suggested in legal doctrine,[33] the E-Commerce Directive seems to classify Internet intermediaries as a sub-genre of information society service providers. Although they share the basic attributes of the latter, intermediaries are a distinct category specially regulated in Section 4 of the E-Commerce Directive and their operations have to fall in one of three distinct categories provided for in that section: mere conduit, caching or hosting.[34]

Although narrower than the notion of information society service providers, the Internet intermediaries located in Articles 12–14 of the E-Commerce Directive cover a rather wide and diverse universe of network activities, ranging from plain Internet access providers (mere conduits) to more complicated operators with expanded network functionalities (hosts). Caching, which has so far been proven much less controversial than its other two counterparts, seems to represent the middle point of the E-Commerce intermediaries taxonomy.

In contrast to the more detailed DMCA, which lists a broader corpus of activities as privileged intermediary functions,[35] the three genres of the E-Commerce

[30]Which states that: "Liability for activities in the network environment concerns not only copyright and related rights but also other areas, such as defamation, misleading advertising, or infringement of trademarks, and is addressed horizontally in 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 ("Directive on electronic commerce") (4), which clarifies and harmonizes various legal issues relating to information society services including electronic commerce. This Directive should be implemented within a timescale similar to that for the implementation of the Directive on electronic commerce, since that Directive provides a harmonized framework of principles and provisions relevant, inter alia, to important parts of this Directive. This Directive is without prejudice to provisions relating to liability in that Directive."

[31]Which provides that: "The Community provisions governing the substantive law on intellectual property, Directive 95/46/EC, Directive 1999/93/EC or *Directive 2000/31/EC, in general, and Articles 12 to 15 of Directive 2000/31/EC in particular.*" (emphasis added).

[32]Case C-70/10, Scarlet Extended, par. 30–35. In the same line, see Van Eecke (2011), p. 1488.

[33]Riordan (2016), Chapter 2, Section 2.

[34]CJEU, Case C-291/13, Sotiris Papasavvas, par. 38–39.

[35]For a closer examination of the intermediaries privileged under the DMCA see Band and Schruers (2002), pp. 295–320; Evans (2004), pp. 445–499; Lemley and Reese (2004),

intermediaries (mere conduits, caching operators and hosts) appear at first limited, especially if one takes into account that they were designed and adopted before the breakthroughs of Web 2.0 that have heavily transformed the landscape of Internet communications. Important online service providers such as search engines, online and mobile market places and user generated content web hosts seem thus not to fit in the intermediary classifications of EU Law. The CJEU had to address such ambiguities in two cases: in Google France[36] the Court had to examine whether Google could enjoy the E-Commerce liability immunities for its AdWords function and in L'Oreal v. eBay[37] it was an online auction operator that was put in close examination.

Although in both cases the Court avoided to express a definite opinion on the subject matter, bestowing that duty upon the national courts that made the references, it came up with a dynamic, flexible and practical doctrine[38] that seems to be the common foundation of the dogmatic depth of the European notion of "Internet intermediaries." In that regard, the Court has used Recital 42 of the E-Commerce Directive on the basis of its analysis[39] and declared that[40]:

> …it follows from recital 42 in the preamble to Directive 2000/31 that the exemptions from liability established in that directive cover only cases in which the activity of the information society service provider is 'of a mere technical, automatic and passive nature,' which implies that that service provider 'has neither knowledge of nor control over the information which is transmitted or stored.'

That analysis suggests that the common thread that tailors together the notion of "intermediary" in EU law is the neutral nature of the operations of a service provider, consisting of merely technical, automatic and passive interventions[41] in the

(Footnote 35 continued)

pp. 1345–1434; Walker (2004), pp. 1–23. For an insightful comparative analysis of EU and US law in general see Peguera (2009), pp. 481–512.

[36]Joined cases C-236/08 to 238/08.

[37]Case C-324/09.

[38]For a similarly positive account see Guadamuz (2014), p. 320.

[39]Recital 42 of the E-Commerce Directive provides that: "The exemptions from liability established in this Directive cover only cases where the activity of the information society service provider is limited to the technical process of operating and giving access to a communication network over which information made available by third parties is transmitted or temporarily stored, for the sole purpose of making the transmission more efficient; this activity is of a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored."

[40]Joined cases C-236/08 to 238/08, Google France, par. 113, case C-324/09, L'Oreal v. eBay, par. 112.

[41]Kohl (2013), pp. 187–234, has provided some interesting argumentation in pointing out that a mere technical, automated and passive Internet service is not always neutral in the sense of the case law of the Court, using the search engine operation of Google as an underlying example. She nonetheless seems to admit that putting the burden of a primary liability in the shoulders of Google is not an alternative and recognizes that Google is already functioning as a diligent gatekeeper, willing to cooperate with the copyright industry rather than opposing it.

dissemination of information within a digital network.[42] Established on that common background the three genres of intermediaries nestled down in Articles 12–14 of the E-Commerce Directive could probably be understood not as closed and independent intermediary classifications, but as interrelated intermediary phenotypes that can embrace the different variations of the evermore complicated intermediary ecosystem. While the mere conduit phenotype seems more suitable to cover mere passive and technical functionalities, the host phenotype can cover more advanced, complicated and creative operations that require a higher degree of involvement in the distribution process without amounting to an independent production, knowledge, control and management of it.[43]

That general and technologically neutral assessment of the CJEU that puts the neutral role of an Internet service provider at the core of its analysis, allows EU Law to accommodate all kinds of Internet operators such as search engines,[44] hyperlinking sites,[45] mobile commerce portals,[46] user generated content hosts,[47] etc., to be flexibly measured within the intermediary phenotypes of Articles 12–14 of the E-Commerce Directive. Depending on the level of their involvement in the process of distribution of information they can be classified as mere conduits or hosts accordingly. The neutrality test of the CJEU will offer the upper limit of their involvement. Exceeding that limit would mean that they no longer merely distribute but that they actively control, produce and manage the information that is disseminated within a network and that they therefore are no longer intermediaries.

The recent ruling of the CJEU in McFadden[48] verified the dynamic and flexible nature of the Court's analysis regarding the notion of Internet intermediaries. One

[42]Van Eecke (2011), pp. 1481–1484, criticized that all-encompassing approach of the Court that puts at the core of its analysis the neutrality of the role of intermediaries, on the basis that while mere conduits and caching operators are indeed neutral service providers, content hosts must, by their nature, perform actions that presuppose some degree of involvement with the users, even if they must still keep some distance from the latter in order to avoid primary liability. While there is much reasonableness in that analysis, it seems that it misses the core argument of CJEU: the neutral role of the Internet service providers is not to be measured only on their function per se, but it must also be projected on their participation in the production of information. It is the knowledge and control of information that would take them out of the realm of intermediaries not the mere distribution of it, even if they are relatively highly involved in it.

[43]CJEU, Joined cases C-236/08 to 238/08, Google France, par. 114 and 120.

[44]For the problem of treating search engines as intermediaries, see Bohan (2006), pp. 181–228; Fitzgerald et al. (2008), pp. 103–120; Synodinou (2010). For comparative considerations from the perspective of US law, see Gasser (2006), pp. 201–234.

[45]Linking has not yet arrived as a problem of Internet intermediaries before the CJEU. In the recent Svensson (C-466/12) and GS Media cases (C-160/15) the Court examined the problem of linking within the limits of the right to communication to the public of Article 3 InfoSoc Directive. See further on that Buri (2014), pp. 245–255.

[46]For a detailed assessment of whether mobile market operators can be treated as intermediaries within Articles 12 to 14 of the E-Commerce Directive, see Jakobsen (2010), pp. 29–52.

[47]For the problem of classification of user generated content hosts as intermediaries, see Hoeren (2009), pp. 1–19; Valcke and Lanaerts (2010), pp. 119–131.

[48]Case C-484/14.

of the main questions in that case was whether a business that sells lighting and sound systems and offers, as part of its marketing strategy, anonymous access to a wireless local area network could be classified as an intermediary within the meaning of Article 12 of the E-Commerce Directive. After verifying that such access to a communication network must not go beyond a technical, automatic and passive process,[49] the Court stated that offering access to a Wi-Fi network is an operation classified as mere conduit in the meaning of Article 12 of the E-Commerce Directive, irrespective of whether there is a contractual relationship between the user and the access provider.[50] It is thus clear that the pallet of intermediaries against which copyright holders can seek injunctions is rather colorful. As such, the outer limits of their dogmatic depth shall be traced in the intermediary phenotypes of Section 4 of the E-Commerce Directive, under the authoritative guidance of the relevant case law of the CJEU that has been presented above.

2.3 *The Practical Significance of the Personal Scope of Application*

The exploration of the personal scope of the injunctive remedies against Internet intermediaries does not have mere dogmatic value. Its practical implications extend to a multilayered spectrum that ranges from the identification of the possible defendants to the appropriateness and legitimacy of the measures that the copyright holders are entitled to apply for.

Such an idea could reasonably be founded in a systematic and comparative interpretation of Articles 12–14 of the E-Commerce Directive. As established previously,[51] the level of involvement of the different intermediary phenotypes in the distribution of information varies. While mere conduits have the lowest level of involvement within a network, host operators display the highest. It is as if the intermediary taxonomy of the E-Commerce Directive runs on a sliding scale, where one end leads to immunity while the other opens the door to primary liability. The intermediary phenotypes of the E-Commerce Directive travel along this sliding scale occupying different positions on it; mere conduits are closer to immunity by virtue of their more neutral role; caching operators occupy the middle point of the sliding scale and, finally, host providers occupy the edge that is closest to liability.

Such a sliding scale effect seems to be reflected on the regulation of the different intermediary phenotypes. According to Article 12 (1) of the E-Commerce Directive, mere conduits can avoid liability if they prove that following conditions were cumulatively met: (a) they did not initiate the transmission of information; (b) they

[49]C-484/14, McFadden, par. 49.

[50]C-484/14, McFadden, par. 50.

[51]See above Sect. 2.2.

did not select the receiver of the transmission; and, (c) they did not select or modify the information contained in the transmission. On the contrary, according to Article 14 (1) the conditions that the host providers must meet in order to claim immunity are more cumbersome. They must prove that they did not have actual knowledge of illegal activities taking place within their operations and also that, upon obtaining such knowledge or awareness, acted expeditiously to remove or disable access to the infringing information. Additionally, as it is further explained in Recital 48 of the E-Commerce Directive, host providers might also be subject to duties of care in order to actively detect and prevent certain types of illegal activities, while mere conduits are exempted from such an obligation.[52]

The privileged treatment of mere conduits in comparison to host providers in terms of the immunity conditions prescribed in the E-Commerce Directive has been recently confirmed in the aforementioned McFadden case.[53] The CJEU was asked whether mere conduits are also obliged to expeditiously remove or block access to information upon obtaining knowledge or awareness of the illegal nature of the latter, in order to maintain their immunity status. Both AG Szpunar[54] and the Court[55] have denied such an extensive interpretation of Article 14 (1) (b), reiterating that the different nature of the operations of mere conduits, which are by definition more technical, automatic and passive and usually have limited duration, in comparison to the wider involvement of host providers in the dissemination of information. This justifies the substantially different treatment of the conditions that secure their immunity from primary liability, according to Articles 12 (1) and 14 (1) of the E-Commerce Directive.[56] As was nicely summarized by AG Szpunar[57]:

> …Articles 12 to 14 of Directive 2000/31 relate to three distinct categories of activity and make the limitation of the liability of providers of the relevant services subject to different conditions, account being taken of the nature of each of the activities in turn. Since the application of those conditions by analogy would have the effect of making the conditions for liability in relation to each of those activities – which the legislature clearly differentiated – the same, it would be incompatible with the general scheme of those provisions…

By the same token, it would seem reasonable and legitimate to extend this line of thinking to the scope of injunctions that can be ordered against Internet intermediaries. On that basis, one should measure the appropriateness of the injunctions ordered against Internet operators according to the nature of activities and the position that each intermediary phenotype occupies within the intermediary system developed in Articles 12–14 of the E-Commerce Directive. While host providers

[52]Recital 48 makes explicitly clear that only host providers might be subject to duties of care, relieving mere conduits and caching operators from such a burden.

[53]Case C-484/14.

[54]See his opinion on case C-484/14, McFadden, par. 97–100.

[55]C-484/14, McFadden, par. 59–63.

[56]For a different approach expressed prior to the ruling of the Court in McFadden, see Savin (2013), p. 114.

[57]Par. 99 of his opinion on case C-484/14, McFadden.

could legitimately be open to more cumbersome, complicated and intrusive injunctions, mere conduits should generally be treated with much more reservation and caution.[58]

Quite surprisingly, however, the CJEU has contradicted itself within the same decision. While it denied that mere conduits should be treated as host providers and act upon notice in order to avoid their primary liability pursuant to Article 14 (1) (b), it has nonetheless (and contrary to the well-founded different opinion of AG Szpunar)[59] accepted that they can be obliged to password protect their connections and request from the users to reveal their identities in order to be granted access to the network.[60] Among several points of the McFadden ruling that raise concerns,[61] it is the profound contradiction in the internal philosophy regarding the intermediary immunities system that shall be highlighted here.

Although it is clear that the immunity regime of Articles 12–14 of the E-Commerce Directive demands a different treatment of mere conduits in comparison to host providers on the basis of the different nature of their activities (a fact recognized by the Court itself already). The farfetched interpretation regarding the scope of injunctive remedies against mere conduits can now be used as a Trojan horse that will hamper the systematic security and internal integrity of the E-Commerce intermediary immunities system. Additionally, despite the explicit exception of mere conduits from duties of care in order to actively detect and prevent certain types of illegal activities, as the latter are neither compatible with their position within an information network nor reasonable on the basis of their technical, automatic and passive role, they might now be forced to apply such duties by virtue of disproportionate injunctions against them.

3 The Procedural Scope of Injunctions Against Internet Intermediaries

3.1 General Overview of the Limits on the Procedural Scope of Injunctions Against Intermediaries

As noted above, although EU law obliges the Member States to allow injunctions against Internet intermediaries for copyright violations, even if the intermediaries are not per se liable, it does not provide for the procedures and modalities that shall

[58]Put in the words of Savvola (2014), p. 118: "…All in all, the differences in the legal basis and the scope when comparing connectivity and hosting providers suggests (sic) that appropriateness of injunctions varies. Because for connectivity providers the conditions for liability exemption are broader, similar limitations could very well also apply to all types of injunctions…".

[59]AG Szpunar on C-484/14, McFadden, par. 134–150.

[60]See C-484/14, McFadden, par. 90–98.

[61]Stalla-Bourdillon (2016).

regulate these measures. The creation of the procedural framework of such injunctions is left to the Member States.

EU law provides nonetheless the lower and upper outer limits of the appropriateness of injunctions against intermediaries. The lower outer limits are traced in the principles of equivalence and effet utile of EU Law,[62] as it is already suggested by Article 3 (2) of the Enforcement Directive. The principles of equivalence and effet utile of the EU law oblige the Member States, when implementing substantive EU law through their national procedural systems, to treat the former appropriately (by tailoring, if necessary, their procedural laws on the special demands of EU substantive law and by treating it equally with their own substantive law) and effectively (by making sure that their procedural laws will be able to give full effect to the provisions of substantive EU law) and allow the CJEU to control whether the Member States have indeed complied with these procedural obligations.[63] As the CJEU confirmed in L'Oreal v. eBay[64]: "Those rules of national law must, however, be designed in such a way that the objective pursued by the directive may be achieved…. In that regard, it should be borne in mind that, under Article 3 (2) of Directive 2004/48, the measures concerned must be effective and dissuasive."

Article 15 of the E-Commerce Directive constitutes another basic limit of the procedural scope of injunctions against intermediaries stemming from EU law. It prevents Member States from imposing general obligations of monitoring or general obligations to actively seek facts or circumstances facilitating illegal activities on Internet intermediaries. As the Commission explained, the basic ratio legis of this limit is the profound impracticality of such measures and the clearly disproportionate burden that they would put on the burdens of intermediaries, as the volume of data that travel through digital networks is vast.[65] What is allowed, however, is monitoring obligations imposed in a specific, clearly defined individual case,[66] although Member State courts have not yet received further instructions on how to implement such individual monitoring measures from the CJEU.

The case law of the CJEU has further provided the upper "outer limit" of the procedural scope of injunctions against intermediaries, that being the fair balance test to which they are ultimately subjected.[67] That test has appeared already in the

[62]See Husovec & Peguera (2015), p. 16.

[63]For a detailed account of the case law of the CJEU that established the procedural projections of the principles of supremacy and effet utile, see Storskrubb (2008), pp. 13–32; Galetta (2011), pp. 33–74.

[64]Case C-324/09, L'Oreal v. eBay, par. 136.

[65]First Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee of 21 November 2003 on the application of Directive 2000/31/EC on electronic commerce, COM (2003)702 final, p. 14.

[66]First Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee of 21 November 2003 on the application of Directive 2000/31/EC on electronic commerce, COM (2003)702 final, p. 14.

[67]Husovec & Peguera (2015), pp. 17–20, who put this test of the CJEU in closer scrutiny and explore its possible limits.

mid-2000's in the case law of the CJEU related to information seeking measures requested against intermediaries. In Promusicae[68] and Tele2[69] the Court established that although EU law seeks to facilitate a strong copyright enforcement regime through the InfoSoc and Enforcement Directives, the protection of copyright must not take place at the expense of other fundamental rights protected in the EU,[70] albeit it avoided to offer concrete guidance on how to perform such a balancing test in these early cases.[71]

The concretization of that balancing test as well as of the other limits on the procedural scope of injunctions against intermediaries is an ongoing process of the case law of the CJEU. The following lines will try to summarize the key points of that ongoing development.

3.2 The Procedural Scope of Injunctions Against Intermediaries in the Case Law of the CJEU

3.2.1 Episode 1: Turn Intermediaries into "Police"

The first measure that caused much controversy and discussion in the EU has been court injunctions that required from Internet intermediaries to install filtering and blocking systems at their own expense, indiscriminately monitoring all electronic communications of all their customers passing via their services, as a preventive measure for an unlimited period of time. Several opinions in the legal literature[72] have put the measures under closer scrutiny and have pointed out the negative effect that they would have on the Internet ecosystem, shall they be found compatible with EU law. It has thus been submitted that such measures are in clear contrast with the prohibition of general monitoring measures prescribed in Article 15 of the E-Commerce Directive,[73] which aims to prohibit Member States from adopting such blanket measures against intermediaries.

It has also been suggested that such measures interfere strongly with multiple other fundamental rights and their implementation would fall short from achieving a

[68]Case C-275/06.

[69]Case C-557/07.

[70]Promusicae, Case C-275/06, par. 63–65, Tele2, case C-557/07, par. 28.

[71]The CJEU transferred that obligation to the national legislators, whom bestowed with the duty to transpose in their domestic legal orders the different EU Directives aiming to protect fundamental EU rights in a way that would satisfy the ends of all of them. See Promusicae, case C-275/06, par. 68 and Tele2, case C-557/07, par. 28. For an insightful analysis of the balancing tests applied by the CJEU and the ECtHR see Angelopoulos (2015), pp. 72–95. For a comparative analysis of the EU balancing system with the corresponding value system of the DMCA see Stalla-Bourdillon (2010).

[72]See Angelopoulos (2009), pp. 1–11.

[73]See Montero and Van Enis (2011), pp. 22–35.

fair balance between copyright and the other competing rights. On the one hand, with the right of Internet intermediaries to conduct business, established in Article 16 of the Charter of Fundamental Rights of the EU; if the intermediaries install such a filtering system as the requested at their own expenses, they are automatically (and rather unwillingly) turned into permanent partners of the copyright holders, a kind of a private copyright "police," that does not share in the benefits of that policing. In addition, the installation, control and management of such a system on a permanent basis and for an unlimited period of time would require a huge logistical and economic effort, distorting the normal business model of Internet intermediaries and consuming much of their resources for activities that are foreign to their basic functions. On the other hand, the rights of the users are equally distorted. First and foremost, their rights to private life and the protection of their personal data, established in Articles 7 and 8 of the Charter, would be severely damaged, as the requested filtering system does not offer enough guarantees securing the integrity of these rights. In addition, their right of freedom of expression would also be affected as:

> a combined filtering and blocking system will inevitably affect lawful exchanges of content, and will therefore have repercussions on the content of the rights guaranteed by Article 11 of the Charter, if only because the lawfulness or otherwise of a given communication, which depends on the scope of the copyright concerned, varies from country to country and therefore falls outside the sphere of technology. So far as it is possible to judge, no filtering and blocking system appears able to guarantee, in a manner compatible with the requirements of Articles 11 and 52 (1) of the Charter, the blockage only of exchanges specifically identifiable as unlawful.[74]

Finally, it has been submitted that the right of users to a fair trial[75] would also be violated, as the filtering and blocking systems affecting their private life, right to data protection and freedom of expression are usually adopted in court proceedings in which they are not taking part.[76]

The CJEU had to address the conformity of such injunctions with EU law in the twin cases Scarlet Extended[77] and Sabam v. Netlog.[78] The outcome was not surprising, as the Court verified the profound incompatibility of such general filtering and blocking systems with EU law. What has been surprising, however, was the Court's reasoning and justification. Unlike its usual minimalistic approach and despite the fact that it already declared such filters incompatible with Article 15 of the E-Commerce Directive,[79] the Court went on further to test whether the

[74]Opinion of AG Cruz Villalón, case C-70/10, Scarlet Extended, par. 86. See also Smith (2010), pp. 88–95; Geiger and Izyumenko (2014), pp. 316–342.

[75]Art 47 (2) of the Charter of Fundamental EU Rights.

[76]For a penetrative analysis of the fundamental user rights affected by such general monitoring and blocking filters, see Neri (2011), pp. 1–13, esp. 9–13. For the problem of the procedural absence of users see also Husovec & Peguera (2015), pp. 28–30.

[77]Case C-70/10.

[78]Case C-360/10.

[79]Scarlet, case C-70/10, par. 40, Sabam v. Netlog, case C-360/10, par. 38.

requested filters could survive a balancing test, that being one of the first of the kind to be conducted by the CJEU itself. After a close examination of the affected fundamental rights of the intermediaries and the users, the Court came to the undisputed conclusion that imposing on Internet intermediaries the adoption of a general and permanent filtering system at their own expenses, would fall short of striking a fair balance between the protection of copyright and the protection of intermediaries and users rights (freedom to conduct business, right to private life and to data protection and freedom of expression), as the scale would in such a case lean only in favor of copyright to the detriment of the other rights.[80]

The Scarlet Extended and Sabam v. Netlog case law has thus contributed to the creation of a more coordinated and concrete EU balancing test that could offer better guidance to the legislators and judges of the Member States in their effort to create an EU conform procedural framework for injunctions against intermediaries.[81] What that case law has left open, nonetheless, is the issue of when and under which circumstances could Member States legislators, authorities or courts impose monitoring obligations on Internet intermediaries. Apart from declaring that general filtering and blocking systems like those examined in Scarlet Extenden and Sabam v. Netlog are incompatible with Article 15 of the E-Commerce Directive, the Court did not explore if, and under which premises, such systems might be found compatible with EU law in individual cases. It is thus left to Member States or future CJEU case law to deliver on these questions.

3.2.2 Episode 2: Turn Intermediaries into Judge, Juries and Executioners

The declaration of general monitoring and blocking filters as incompatible with EU law has directed the interest of copyright holders to other solutions. The next trend that started to flourish was that of injunctions requesting Internet intermediaries to block access to websites that have been assumed to facilitate copyright violations. The blocking trend has been proven equally (if not more) controversial.

There are several legitimate objections that are raised against website blocking as a measure to curb online copyright violations. A first category of concerns stems from the rather diverse and complex technical ways of implementing the measure. There are currently three methods of website blocking: the most simple is the so called "DNS blocking" and requires the service providers to change the configuration of their DNS servers in order to bar certain domain names from their DNS logs; "IP blocking," another method, hinders the access to certain websites by blocking data packets with a certain destination address; finally, the most complicated type of blocking is called "URL blocking" and unlike the other two requires

[80]Scarlet, case C-70/10, par. 44–54, Sabam v. Netlog, case C-360/10, par. 44–51.

[81]For the importance of the balancing test conducted in the examined cases, see Roth (2012), pp. 125–128.

that the service provider inspects, apart from the headers of IP packets, the contents of the latter.

Each one of the aforementioned methods comes with its own individual problems when translated into an injunction against an intermediary. "DNS blocking" is usually considered to lack effectiveness, as it appears to be easily circumvented both by the service providers (by using another domain name) and by the users (by searching for alternative DNS servers). "IP blocking" has also been considered not particularly effective, as at least the service providers can easily circumvent it by obtaining a new IP address. Additionally, it seems to raise serious concerns about its proportionality, as it can lead to excessive blocking: taking into account that IP addresses are used by numerous websites, there is no guarantee that websites not related to any violations will still not be affected by it. Similar objections are also raised against "URL blocking," especially if attention is drawn on the huge logistic and economic sacrifices that the website operators are subjected to in order to comply with it.[82]

Low effectiveness and lack of proportionality are not the only issues that could put the compatibility of blocking injunctions with EU law in question. Such measures also seem to interfere with several fundamental rights of the intermediaries and the users. Regarding the intermediaries, it is their freedom to conduct business that comes first in question. Imposing blocking measures would require consuming considerable (depending on the method of blocking) time, effort and resources, a sacrifice that does not belong in the usual costs that an Internet intermediary is subjected to in the course of their normal activities. Moreover, it has been observed that Internet operators subject to blocking injunctions might be hindered from performing their core social role, namely that of regulating the amount and quality of information disseminated within their networks (as blocking measures will severely interfere with that process), raising thus issues that affect the protection of the freedom of expression and information (Article 11 of the Charter), although at the same time such restrictions will, of course, be projected on the corresponding rights of their customers.[83] Users might be further hindered from accessing information if they have to face higher subscription prices because of the implementation of blocking measures. Finally, as is the case with filtering systems, the users' right of fair trial seems not to be observed. Once more they will not have the opportunity to be part of the court proceedings adjudicating over the blocking injunction, although their legal position (due to the possible violation of their fundamental rights of freedom of expression and information) is strongly affected by them.[84]

[82]For a detailed overview of the technical preconditions and the effectiveness and proportionality of the basic blocking methods. See Feiler (2012), pp. 6–11.

[83]Opinion of AG Cruz Villalón, case C-314/12, UPC, par. 82.

[84]For a complete analysis of the impact of blocking measures in terms of their effectiveness, proportionality and their interference with fundamental rights of the intermediaries and the users, see Husovec (2013), pp. 116–126.

The CJEU had the opportunity to examine the aforementioned issues in the UPC case.[85] It must be noted that the case was tailored around the particularities of Austrian law, which allows a court, upon the request of a copyright holder, to order intermediaries to block websites, without specifying the preconditions and modalities for achieving that result. That particularity blurs the problems attached to effectiveness, proportionality and fair balancing. Taking into account that such a general court order does not offer enough space for considerations of that kind and it is prone to legal uncertainty.

Despite the different opinion of Advocate General Villalón, who found that the outcome prohibitions of Austrian law obliging Internet intermediaries to block access to certain websites without providing for the concrete preconditions of that blocking do not strike a fair balance (even if the intermediary can claim at a later procedural stage that he took all reasonable measures possible in order to implement the blocking in order to avoid liability),[86] the Court ruled that they are compatible with EU law. The flexible nature of the outcome prohibitions and the fact that the intermediaries can, according to the Court, implement the blocking choosing the method that is best suited to their abilities and resources, have been found not to violate the core substance of the intermediaries right to conduct business and allow, therefore, the striking of a fair balance between that right and the protection of copyright.[87] Interestingly, the Court did not interfere in the balancing process between copyright and the rights of the users affected by website blocking. That duty was bestowed directly upon the intermediaries[88] who are therefore obliged to find a formula that satisfies the need to protect copyright, without hampering their business model and the users' rights to freedom of expression and information. Despite avoiding a closer inspection of the balancing issues surrounding blocking injunctions, the Court offered a general assessment of their effectiveness, by lowering its expectations in that regard. Even if the blocking measures adopted by an intermediary in the context of an outcome prohibition do not amount to full satisfaction of the copyright holder, they will still be compatible with EU law, provided that they at least make the violation of copyright protected works harder or seriously discourage such a violation.[89] The motive of the Court behind the establishment of such low expectations in terms of the effectiveness of blocking injunctions is unclear.

In UPC the CJEU displayed a tendency to diplomatically avoid a deeper analysis of the most controversial aspects of website blocking. It has in fact delegated the

[85]Case C-314/12.

[86]AG Cruz Villalón, case C-314/12, UPC, par. 85–90.

[87]Case C-314/12, UPC, par. 50–52.

[88]Case C-314/12, UPC, par. 56.

[89]Case C-314/12, UPC, par. 62.

very delicate balancing process to the intermediaries themselves,[90] without offering sufficient guidance to them. That is a huge burden if one pays attention to the fact that Internet operators are neither judges nor can all of them have access to legal counseling on that level. The ruling of the Court is also possible to create a new wave of legal uncertainty within the common digital market, because by delegating the balancing test to the intermediaries it has opened the possibility of as many different balancing interpretations as the Internet operators across the Member States. Finally, the questions of whether blocking injunctions shall have a general or a specific nature has been left rather unclear, as the Court did not elaborate much on that direction, apart perhaps from stating that blocking measures must be of a specific nature in order not to violate the users' right of freedom of information.

3.2.3 Episode 3: Turn Passive Mere Conduits into Active Copyright Enforcers

The last episode of the intermediary injunctions case law of the CJEU refers to the fate of open Wi-Fi spots. Among other interesting issues of Internet intermediary regulation in the EU,[91] the Court has been asked in the recently published McFadden case[92] whether a business that offers as ancillary to its principal, non-Internet related activities, Internet access via an open Wi-Fi network could be obliged via an injunction to either terminate its entire connection point or examine all the communications transmitted through it or, finally, password protect its connection in order to stop violations of copyright allegedly committed within its network.

As already explained above, the Court has classified the operators of an open Wi-Fi spot as mere conduits within the meaning of Article 12 of the E-Commerce Directive. That automatically means that the injunctions requested by the right holders in the McFadden case, shall survive the scrutiny of the common limitations established in the previous case law of the CJEU in order to be deemed compatible with EU law.

While terminating the operations of the open Wi-Fi spot is a clear violation of the core essence of the right to conduct business, even if the latter is exercised in an ancillary manner, and, monitoring the entire communications going through it is an undisputed violation of Article 15 of the E-Commerce Directive, causing thus no

[90]Angelopoulos (2014), p. 818 notes: "…According to the court, the right solution is the one that keeps everybody happy, while the hot potato of how this might be achieved is tossed to the intermediaries. Internet access providers must thus make sure that both right holders and users are served the whole of the same cake with no real guidance as to what measures might achieve that effect…".

[91]Most notably the compatibility of the German copyright law "Störerhaftung" doctrine with the intermediary regime of Articles 12–14 of the E-Commerce Directive, for which see Nordemann (2011), pp. 37–46; Frey et al. (2012), pp. 1–26.

[92]Case C-484/14.

disparities between AG Szpunar and the Court,[93] the password protection of the Wi-Fi access point has been more controversial and required a more detailed analysis.

AG Szpunar presented very strong reasons against its compatibility with EU law.[94] First of all, he pointed that forcing open Wi-Fi operators to password protect their connections would severely interfere with their right to conduct business, given that if faced with the additional costs and efforts attached to the management of the password system, they might desist from operating it. He stressed, further, that a password system would be effective in terms of copyright enforcement, if the Wi-Fi operator registers the users and retains their personal data, as this will allow the identification of the alleged infringers by the right holders. He found such an additional interference with the business model of the Wi-Fi access providers clearly disproportionate.[95] Finally, he expressed serious and substantial doubts about the effectiveness of the measure, as password locking would limit the circle of users but not necessarily prevent copyright infringements and he found that such a measure would ultimately be a major disadvantage for society overall and one that could outweigh the benefits for right holders, especially on the grounds of recognizing an innovation potential on open Wi-Fi access.

It could be added to that argumentation that especially the obligation of the Wi-Fi operators to register and retain the personal data of their users, constitutes a severe intrusion in the rights of private life and data protection of the latter, as it would force them to identify themselves in order to gain access to the network and it would force the operators to check and validate the users' identity. Additionally, the obligation of users to reveal their identity (even via an email address) might discourage them from accessing the network and therefore also interfere with the rights of freedom of expression and information.

The Court did not follow the opinion of AG Szpunar and decided that forcing Wi-Fi access providers to password protect their network is compatible with EU law. It based that conclusion firstly on the assumption that password protection of Wi-Fi networks does not interfere both with the core substance of the right of the Wi-Fi providers to conduct business (as it only presupposes a trivial setting on their system requirements) and with the core substance of users' freedom of information (as the users can always access the Internet from other networks).[96] It is

[93]See the opinion of AG Szpunar, case C-484/14, McFadden, par. 131–132 and the ruling of the Court in the same case par. 87–88.

[94]AG Szpunar, case C-484/14, McFadden, par. 134–150.

[95]In that regard, it would not be unreasonable to suggest that forcing the Wi-Fi operators to register their users and retain their personal data would probably make them data controllers or processors, imposing on their shoulders the efforts and costs required in order to comply with the data protection law obligations and safeguards attached to such a role. For the circumstances and conditions that would bring Internet intermediaries to the realm of data protection compliance, see Van der Sloot (2015), pp. 216–219.

[96]C-484/14, McFadden, par. 91–92.

questionable whether these arguments can survive the scrutiny presented by AG Szpunar.

The Court examined, further, the effectiveness of password protecting a Wi-Fi network and concluded that mere password locking cannot even meet the low threshold established in UPC (that being that it is enough if copyright infringements are becoming more difficult if they cannot be averted at all) if it is not combined with user registration and identification.[97] Despite the obvious interference of such registration and identification obligations with the users' right to private life and to data protection, the Court did not assess the occurring problems, making thus its reasoning weaker. Finally, the Court stressed[98] that if password protection of the operators' network is denied, the copyright holders right to intellectual property would be denied any protection, taking into account that the other suggested measures, namely terminating the operation of the network and monitoring all the communications passing through it, have been rejected. That is a rather weak and arguable point. Injunctions against intermediaries are not the only procedural remedy prescribed by EU law in favor of the right holders. The Court seems to pretend that the rest of the quite lucrative procedural rights established for the sake of copyright holders in the Enforcement Directive do not exist.[99]

The McFadden ruling seems to put the model of open Wi-Fi access in serious question. More generally, it represents an example of a rather strong shift of the CJEU case law towards a stricter copyright enforcement regime and a clearly more active involvement of Internet intermediaries (even mere conduits) as private copyright enforcers,[100] without providing convincing justifications for such a move. It remains to be seen if that shift will be permanent or whether another change of the tide might occur in the future.

4 Conclusion

The European injunction system against, otherwise non-liable, intermediaries for the sake of copyright enforcement is still a work in progress, albeit with some distinguishable traits. EU law seems to recognize the sensitive role of intermediaries and to understand the complexity of the issues attached to their involvement in the realm of copyright enforcement. For its part, the CJEU is putting much effort to identify the lower and upper limits of the intermediary injunction phenomenon, although not always successfully. It seems as if the "effectiveness," "proportionality" and "balancing" tests devised by the CJEU are lacking a central common

[97]Par. 96.

[98]Par. 98.

[99]For an overall assessment of the McFadden ruling, see Husovec (2016a).

[100]Such a shift has been monitored globally already at the end of the previous decade. See Beer and Clemmer (2009), pp. 375–409.

thread and that they are very much tied in a case by case analysis unable to produce a much-needed unified approach. The EU law injunctions against, otherwise non-liable, intermediaries seem to still be suffering from legal uncertainty, a situation that might have detrimental effects to the free development of innovation and new technologies in the common market.[101]

In search of a more general yet at the same time more balanced approach than the one currently derived from the case law of the CJEU, many commentators[102] are trying to identify whether the system of ordering injunctions against non-liable intermediaries can meet an optimal standard, one that shall, at the very end, achieve the best promotion of all the involved interests. Other commentators propose to move from injunctions to a unification of secondary copyright liability within the EU,[103] while others present reasonable argumentation in the direction of a more open and inclusive digital copyright economy, where copyright holders will make use of innovative business models that can enable their industries to thrive using the Internet technology as an ally and not as an enemy or police.[104]

And while it seems very possible that the current intermediary liability and injunction system will stay with us (at least in the core of its current form)[105] in the near future, there might be an unexplored and very scarcely mobilized potential within the core of EU law itself that could probably substantially optimize the injunction ecosystem. In lack of a unified European civil procedural law, that potential is to be traced within the unifying power of the Charter of Fundamental Rights in regards to the national civil procedural laws of the Member States. After all, the national civil procedural legislators are the main addressees of the EU law mandates regarding injunctions against non-liable intermediaries.

In identifying the basic strategy and underlying principle of the development of EU civil procedural law in the mid 2000's the EU Council stressed[106]:

> …Fundamental Rights, as guaranteed by the European Convention on Human Rights and the Geneva Convention on Refugees, must be fully respected. At the same time, the programme aims at real and substantial mutual confidence and promoting common policies to the benefit of all our citizens….

[101]See the interesting analysis of Ahlert et al. (2004), who display in a rather illustrative way that the legal uncertainty regarding intermediary liability and injunction schemes for violations of third parties within the EU provides an incentive to intermediaries to indiscriminately censor or remove material from the Internet, endangering the neutral character of the latter.

[102]See, e.g., the meticulous analysis of Husovec (2016b).

[103]Angelopoulos (2013); Leistner (2014), pp. 75–90.

[104]See for that argumentation Edwards (2010), pp. 62–70.

[105]See Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM (2016) 288 final. In defense of the current intermediary liability and injunctions system against its modification towards a stricter copyright enforcement instrument. See Rosati (2016).

[106]The Hague Program: Strengthening Freedom, Security and Justice in the European Union, EE C 53 from 03.03.2005, p. 2.

That proclamation could be considered as signaling an interesting shift in the basic mission of the national civil procedural laws. They are no longer the enforcement agents that shall secure the proper functioning of the common market, but they must be further understood as the guardians of fundamental EU rights.

Thus, the binding effect of the Charter of Fundamental Rights proclaimed in Article 6 TFEU could be translated in two separate mandates addressed towards the national civil procedural laws of the Member States. The first one refers to the unifying effect of the right to a fair trial, established in Article 47 (2) of the Charter, and demands the formation of a common EU civil procedural value system (prescribed now not only by the principles of equivalence and effet utile, but also by the basic guaranties of Article 47 (2), namely that Court proceedings shall be conducted by an independent and impartial tribunal, in a fair and public hearing and within reasonable time) at the basis of the administration of civil justice through the national civil procedural systems of the Member States.[107] The second one refers to the internal integrity of the fundamental rights of the EU and bestows upon the national judges the duty to guard them within the general common procedural framework established by Article 47 (2) of the Charter.

Transferred in the case of injunctions against non-liable Internet intermediaries these two mandates would not only mean that the right to a fair trial per se shall be observed, but also that the national civil procedural laws of the Member States shall guarantee that the protection and balancing of the affected fundamental rights (intellectual property, right to conduct business, freedom of expression and information, right to private life and to data protection, etc.) is the underlying principle that shapes the procedural preconditions and modalities of the injunction system on its very basis. Instead of leaving the problem of balancing to be treated at the highest level as an issue of conflict of fundamental rights, the national civil procedural laws of the Member States shall make sure that the procedural modalities regulating the injunctions against non-liable intermediaries secure that all the affected fundamental rights are equally observed, protected and—if necessary—ultimately balanced.

It is in this context that one can better understand the ruling of the Court in Bonnier Audio,[108] and also the mandate of the Court towards national procedure legislators in UPC to "…provide a possibility for Internet users to assert their rights before the court once the implementing measures taken by the Internet service provider are known."[109]

---

[107]In that regard, see Hess (2014), pp. 227–228.

[108]Case C-461/10, par. 59–60, where it was stated: "Thus, that legislation enables the national court seised of an application for an order for disclosure of personal data, made by a person who is entitled to act, to weigh the conflicting interests involved, on the basis of the facts of each case and taking due account of the requirements of the principle of proportionality… In those circumstances, such legislation must be regarded as likely, in principle, to ensure a fair balance between the protection of intellectual property rights enjoyed by copyright holders and the protection of personal data enjoyed by Internet subscribers or users."

[109]Case C-314/12, par. 57 in fine.

Acknowledgements The author would like to thank the Onassis Foundation for supporting his PhD research since 2014.

References

Ahlert Ch, Marsden Ch, Yung Ch (2004) How 'Liberty' disappeared from cyberspace: the mystery shopper tests Internet content self-regulation. http://pcmlp.socleg.ox.ac.uk/wp-content/uploads/2014/12/liberty.pdf. Accessed 8 Oct 2016

Angelopoulos Ch (2009) Filtering the Internet for copyright content in Europe. IRIS Plus 4:1–12

Angelopoulos Ch (2013) Beyond the safe harbours: harmonising substantive intermediary liability for copyright infringements in Europe. http://www.ivir.nl/publicaties/download/1087. Accessed 8 Oct 2016

Angelopoulos Ch (2014) Are blocking injunctions against ISPs allowed in Europe? Copyright enforcement in the post-Telekabel EU legal landscape. J Intellect Prop Law Pract 9(10): 812–821

Angelopoulos Ch (2015) Sketching the outline of a ghost: the fair balance between copyright and fundamental rights in intermediary third party liability. Info 17(6):72–96

Baistrocchi P (2002) Liability of intermediary service providers in the EU directive on electronic commerce. Santa Clara High Technol Law J 19(1):111–130

Band J, Schruers M (2002) Safe harbors against the liability hurricane: the communications decency act and the digital millennium copyright act. Cardozo Arts Entertain Law J 20:295–320

Beer J, Clemmer Ch (2009) Global trends in online copyright enforcement: a non-neutral role for network intermediaries? Jurimetrics 49(4):375–409

Bohan F (2006) Liability of Internet search engines. Hibernian Law J 6:181–227

Bright J, Agustina J (2013) Mediating surveillance: the developing landscape of European online copyright enforcement. J Contemp Eur Res 9(1):121–137

Buri M (2014) Permission to link-making available via hyperlinks in the European Union after Svensson. Jipitec 5:245–255

Cobia J (2009) The digital millenium copyright act takedown notice procedure: misuses, abuses, and shortcoming of the process. Minn J Law Sci Technol 10(1):387–411

Edwards L (2005) Articles 12-15 ECD: ISP liability. The problem of intermediary service provider liability. In: Edwards L (ed) The new legal framework for E-commerce in Europe. Hart Publishing, Oxford

Edwards L (2010) Role and responsibility of Internet intermediaries in the field of copyright and related rights. http://www.wipo.int/export/sites/www/copyright/en/doc/role_and_responsibility_of_the_Internet_intermediaries_final.pdf. Accessed 8 Oct 2016

Edwards L, Waelde Ch (2005) Online intermediaries and copyright liability. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1159640. Accessed 8 Oct 2016

Evans E (2004) From the cluetrain to the panopticon: ISP activity characterization and control of internet communications. Mich Telecommun Technol Law Rev 10:445–499

Feiler L (2012) Website blocking injunctions under EU and U.S. Copyright Law—Slow death of the global internet or emergence of the rule of national copyright law? Transatlantic Technology Law Forum, TTLF Working Papers 13:1–76

Fitzgerald B, O'Brien D, Fitzgerald A (2008) Search engine liability for copyright infringement. In: Spink A, Zimmer M (eds) Web search, Springer Series in Information Science and Knowledge Management 14. Springer, Berlin

Frabboni M (2010) File-sharing and the role of intermediaries in the marketplace: National, European Union and international developments. In: Stamatoudi I (ed) Copyright enforcement and the internet. Kluwer Law International, Alphen aan den Rijn

Frey D, Rudolph M, Oster J (2012) Internetsperren und der Schutz der Kommunikation im Internet-Am Beispiel behördlicher und gerichtlicher Sperrungsverfügungen im Bereich des Glückspiel- und Urheberrechts. Multimedia und Recht Beilage 1–26
Galetta U (2011) Procedural autonomy of EU member states: paradise lost? A study on the "functionalized procedural competence" of EU member states. Springer, Berlin
Gasser U (2006) Regulating search engines: taking stock and looking Ahead. Yale J Law Technol 8:201–234
Geiger Ch, Izyumenko E (2014) Copyright on the human rights' trial: redefining the boundaries of exclusivity through freedom of expression. Int Rev Intellect Prop Compet Law 45:316–342
Giblin R (2014) Evaluating graduated response. Columbia J Law Arts 37(2):147–210
Goldsmith J, Wu T (2008) Who controls the Internet? Illusions of a borderless world. Oxford University Press, Oxford
Guadamuz A (2014) Developments in intermediary liability. In: Savin A, Trzaskowski J (eds) Research handbook on EU internet law. Edward Elgar Publishing, Cheltenham
Hess B (2014) Unionsrechtliche Synthese: Mindenstandards und Verfahrensgrundschätze im acquis communitaire/Schlussfolgerungen für European Principles of Civil Procedure. In: Weller M, Althammer Ch (eds) Mindestandards im europäischen Zivilprozessrecht. Mohr Siebeck, Tübingen
Hoeren T (2009) The European liability and responsibility of providers of online-platforms such as 'second life.' J Inf Law Technol (1). http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2009_1/hoeren. Accessed 8 Oct 2016
Holland A et al (2015) NOC Online intermediaries case studies series: intermediary liability in the United States, Berkman Center for Internet & Society. https://cyber.harvard.edu/is2015/sites/is2015/images/NOC_United_States_case_study.pdf. Accessed 8 Oct 2016
Husovec M (2013) Injunctions against innocent third parties: the case of website blocking. Jipitec 4:116–129
Husovec M (2016a) Holey cap! CJEU drills (Yet) another hole in the E-Commerce directive's safe harbors. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2843816. Accessed 8 Oct 2016
Husovec M (2016b) Accountable, not liable: Injunctions against intermediaries. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2773768. Accessed 8 Oct 2016
Husovec M, Peguera M (2015) Much ado about little-privately litigated Internet disconnection injunctions. International Review of Intellectual Property and Competition Law 46:10–37
Jakobsen S (2010) Mobile commerce and ISP liability in the EU. Int J Law Inf Technol 19(1):29–52
Juliá-Barceló R, Koelman K (2000) Intermediary liability in the E-commerce directive: so far so good, but it's not enough. Comput Law Secur Rep 16(4):231–239
Kohl U (2013) Google: the rise and rise of online intermediaries in the governance of the internet and beyond (Part 2). Int J Law Inf Technol 21(2):187–234
Leistner M (2014) Structural aspects of secondary (provider) liability in Europe. J Intellect Law Pract 9(1):75–90
Lemley M, Reese A (2004) Reducing digital copyright infringement without restricting innovation. Stanford Law Rev 56:1345–1434
Lessig L (2006) Code, version 2.0. Basic Books, New York
Marsden C (2011) Network neutrality and internet-service provider liability regulation: are the wise monkeys of cyberspace becoming stupid? Glob Policy 2(1):53–64
Montero E, Van Enis Q (2011) Enabling freedom of expression in light of filtering measures imposed on Internet intermediaries: squaring the circle? Comput Law Secur Rev 27:21–35
Neri A (2011) Ordering intermediaries to implement filtering mechanisms: a controversial measure with dreadful consequences. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1960676 Accessed 8 Oct 2016
Nordemann J (2011) Liability for copyright infringements on the Internet: host providers (content providers)—The German approach. Jipitec 2:37–49
Peguera M (2009) The DMCA safe harbors and their European counterparts: a comparative analysis of some common problems. Columbia J Law Arts 32(4):481–512

Reed Ch (2003) Liability of online information providers-towards a global solution. Int Rev Law Comput Technol 17(3):255–265
Riordan J (2016) The liability of internet intermediaries. Oxford University Press, Oxford
Rosati E (2016) Why a reform of hosting providers' safe harbour is unnecessary under EU copyright law. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2830440. Accessed 8 Oct 2016
Roth H (2012) Überwachungs- und Prüfungspflicht von Providern im Lichte der aktuellen EuGH-Rechtsprechung. Zugleich Anmerkung zu EuGH, Urteil vom 24. November 2011-C-70/10. Zeitschrift für Urheber- und Medienrecht 56(2):125–128
Savin A (2013) EU internet law. Edward Elgar Publishing, Cheltenham
Savvola P (2014) Proportionality of website blocking: internet connectivity providers as copyright enforcers. Jipitec 5:116–138
Schruers M (2002) The history and economics of ISP liability for third party content. VA Law Rev 88:205–264
Smith G (2010) Copyright and freedom of expression in the online world. J Intellect Prop Law Pract 5(2):88–95
Stalla-Bourdillon S (2010) The flip side of ISP's liability regimes: the ambiguous protection of fundamental rights and liberties in private digital spaces. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2321649. Accessed 8 Oct 2016
Stalla-Bourdillon S (2016) The CJEU rules on free access to wireless local area networks in McFadden: the last (?) shudder of Article 15 ECD, the vanishing of effective remedies, and a big farewell to free Wi-Fi! https://peepbeep.wordpress.com/2016/09/15/the-cjeu-rules-on-free-access-to-wireless-local-area-networks-in-mcfadden-the-last-shrudder-of-article-15-ecd-the-vanishing-of-effective-remedies-and-a-big-farewell-to-free-wi-fi/. Accessed 8 Oct 2016
Storskrubb E (2008) Civil procedure and EU law. Oxford University Press, Oxford
Svantesson D (2016) Private international law and the internet, 3rd edn. Wolters Kluwer, Alphen aan den Rijn
Synodinou T (2010) Google versus the law. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1951837. Accessed 8 Oct 2016
Valcke P, Lanaerts M (2010) Who's author, editor and publisher in user-generated content? http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2584916. Accessed 8 Oct 2016
Van der Sloot B (2015) Welcome to the Jungle: the liability of internet intermediaries for privacy violations in Europe. Jipitec 6:211–228
Van Eecke P (2011) Online service providers and liability: a plea for a balanced approach. Common Market Law Rev 48:1455–1502
Walker C (2004) Application of the DMCA safe harbor provisions to search engines. Va J Law Technol 9(2):1–23
Wu T (2011) The master switch—the rise and fall of information Empires. Vintage Books, New York
Zittrain J (2003) Internet points of control. Boston College Law Rev 44(2):653–688

Part III
Digital Evidence

The Collection of Electronic Evidence in Germany: A Spotlight on Recent Legal Developments and Court Rulings

Nikolaus Forgó, Christian Hawellek, Friederike Knoke and Jonathan Stoklas

Abstract The radical change in telecommunications technologies over the last fifteen years has enabled new techniques to lawfully intercept telecommunications and to gather digital evidence. These include covert remote access to data storages and lawful interception prior to communication encryption by hidden software tools. The specific intrusiveness of these measures, specifically their impact on fundamental rights, have been reflected in the decisions of the German Federal Constitutional Court. In particular, the development of the new fundamental right to integrity and confidentiality of IT systems in the judgment of 27 February 2008 has provided modernized constitutional guarantees, leading to the amendment of the legal framework governing *preventive measures*. With the judgment of 16 April 2016 on the constitutionality of these new provisions, the Federal Constitutional Court has countered the expansion of investigative powers through laws or their extensive application, developing essential requirements for covert surveillance measures. The German legal system is characterized by a strict and fundamental distinction between preventive measures (such as crime prevention) and investigative measures (such as criminal investigation). The distinction results in different legal competences of (police) authorities and a distinct legal framework following an altered proportionality assessment. As a result, the safeguards, checks and balances for investigative measures need to be at least as high as those for preventive measures, requiring corresponding amendments of the Code of Criminal Procedure. It is therefore surprising to find that the Code of Criminal Procedure (governing investigative measures) has only undergone minor amendments, such as the introduction of § 100i StPO governing the use of International Mobile Subscriber Identity (IMSI) catchers. The use of covert software to intercept telecommunications prior to encryption, conversely, lacks specific rules, albeit the strict requirements laid down for preventive measures in § 20k BKAG a fortiori should apply on investigative measures of the same nature. Only regarding

N. Forgó (✉) · C. Hawellek · F. Knoke · J. Stoklas
Institute for Legal Informatics, Leibniz Universität Hannover, Hannover, Germany
e-mail: forgo@iri.uni-hannover.de

M. Corrales et al. (eds.), *New Technology, Big Data and the Law*,
Perspectives in Law, Business and Innovation, DOI 10.1007/978-981-10-5038-1_10

computer-assisted searches, the German Federal Supreme Court has ruled in 2007 that such a measure cannot be based upon the existing legal bases for the lack of adequate safeguards. This lack of modernization of the rules applicable to criminal investigation appears unfortunate, as the measures in question, in the view of the authors, should not be based upon the traditional rules designed for physical wire-tapping of telephone lines. Rather, the specific safeguards laid down in § 20l (2) BKAG, such as the requirement to automatically undo alterations imposed upon the infiltrated system, should be codified for investigative measures, as well as to maintain a comparable level of protection of fundamental rights. However, currently there are no signs that the legislator intends to take any steps to amend the corresponding legal framework for investigative measures.

Keywords Digital evidence · Surveillance · Germany · Fundamental rights

Contents

1 Introduction

1.1 Scope and Aim

The move to a digitalization of society has posed new challenges both to Law Enforcement Authorities (LEAs) and to the related legal framework, in particular the implementation of adequate privacy safeguards. Where traditional evidence would be collected onsite as physical evidence, scattered along the crime site by long-established and continuously developed procedures based upon an established legal framework, nowadays telecommunication networks, computers and a large variety of mobile devices are essential for the collection of the evidence needed to successfully investigate a crime. However, there are less established procedures in place as to how to deal with these new forms of investigation.

The need to "go digital" obviously applies to all sorts of cybercrimes, including the various crime types laid down as offences in the Cybercrime Convention,[1] such as illegal access (to IT systems) , data interference, system interference, misuse of devices, computer-assisted forgery and computer-assisted fraud. Moreover, previously existing types of crime have found new domains in digital environments, such as child pornography and all types of infringements of intellectual property rights.

Still, digital evidence likewise becomes more relevant for crimes committed in the physical world, be it trafficking or the illegal trade of narcotics, crimes related to terrorism, money laundering or murder, assault and sexual crimes. In all cases, digital traces recovered from systems, devices and networks can provide valuable information e.g., on the whereabouts of a suspect at the time of the crime, previous communications with other potential offenders, files documenting crimes or financial transactions related to these crimes.

As a result, investigation methods need to be adjusted to these changes. This has a major impact on the legal framework underlying investigative measures. Some measures which can be used to access information (such as computer-assisted search) are of a genuine quality regarding their fundamental rights impact which prevents them from being based on the existing legal bases in the law due to the lack of adequate safeguards corresponding to that specific impact. Others, such as seizure, have remained similar to traditional forms of preservation of evidence from a methodological point of view (an object is being taken from the suspect and subsequently forensically analyzed). However, this preservation creates a new quality of impact on the fundamental rights of suspects, which again requires reflection on adequate safeguards.

This becomes obvious when the seizure of a physical object is compared with the seizure of a data container. In the course of an assault investigation, a knife might be seized, for instance. As with all investigative measures, the impact on the fundamental rights of affected individuals need to be balanced against the general

[1]CoE Convention on Cybercrime, ETS 185, http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561. Accessed 26 September 2016.

public's interest to efficiently solve crimes—i.e., a classic proportionality test. The more severe a crime is, the more likely measures with a large impact on fundamental rights may (still) be proportionate and therefore justified, limited, however, by the essentials of all fundamental rights, which remain inviolable.

In view of these considerations, the impact of seizing a knife in the previous example is confined to the fundamental right to property of the owner. Typically, such a knife would not be of outstanding value, it could easily be replaced (if ownership was legal and a knife of such type meanwhile was needed) and the (possibly temporary) loss of that item could be financially compensated, if the law provided for it. Additionally, the amount of personal information accessible through forensic methods would be limited to possibly a few fingerprints and some genetic information, which might be sensitive information, but limited information in terms of quantity.

However, if a smart phone is seized, the situation changes significantly. The device typically contains personal data reflecting vast parts of the professional and/or private life of its user. Hence, the fundamental rights impacted are not only property rights, but also those related to privacy/data protection and, additionally, potentially the privacy of telecommunications (depending on the case and the legal system). LEAs accessing such device gain control of data vaults that reveal various details on the user and various third parties in very high granularity. Most of the information available would likely not be case-relevant at all, so that further analysis would be needed to identify the relevant pieces of information. Finally, unless the data was mirrored in the Cloud or any type of online service, the loss of the device would mean, for the user, not only the loss of a multi-purpose device, but also the loss of that data (potentially triggering severe consequences, if e.g., the address book had not been backed-up).

This example may underpin the crucial difference of investigative measures in a physical and in a digital environment. Where the impact on fundamental rights (massively) increases when applying measures in the digital world, the safeguards have to rise equally. As a consequence, the existing legal framework needs constant revision.

This chapter examines the German legal situation and its development in recent years. Whereas the legal framework has not been systematically adapted to the challenges outlined, at least with regards to genuinely new measures such as computer-assisted search, German legislation has implemented laws providing for such safeguards—although only for measures with preventive purpose, and not (yet) for investigative measures (details on that principal distinction will be given below). This development has happened mostly independently of European developments (with the exception of data retention, which shall not be covered in this chapter). Moreover, the European legal framework contains very few provisions on the *collection* of digital evidence. The few existing provisions are rooted in the Cybercrime Convention. Simultaneously, the constitutional judicature in Germany has reacted to the outlined development by innovative case law and the development of corresponding legal principles which are interesting to examine, and which, with a few exceptions, have mostly been discussed in the German language only.

More importantly, this development has been accompanied by several remarkable decisions of the German Federal Constitutional Court and the German Federal Supreme Court, further developing and shaping the existing legal framework on data protection in the police sector and even introducing a new fundamental right: the fundamental right to integrity and confidentiality of IT systems. These developments are taken as an opportunity to reflect upon the developments in Germany over the last decade.

1.2 The EVIDENCE Project

The research in this chapter is partly based upon the work of the authors in the EVIDENCE project.[2] The EVIDENCE project is a European research project co-financed by the European Union under Framework Program 7 that addresses various challenges posed by the collection and use of electronic evidence. Leibniz Universität Hannover has contributed to this project inter alia by providing the legal analysis and legal recommendations focusing on data protection.

In that respect, the scope of this chapter is narrower than in the EVIDENCE project in the sense that this chapter shall provide a clear focus on the German situation and does not seek to provide a legal comparison or an analysis of the interlinking of the overarching European legal framework. This focus allows for a more detailed reflection on the German situation, which in that respect will exceed the contribution to the EVIDENCE project, which focused on legal comparison and overarching European law.

2 The German Legal System: The Fundamental Distinction Between Preventive and Investigative Measures

2.1 General Observations on the German Situation

Germany has a relatively long tradition in the protection of personal data, both in legislation and judicature. The state of Hessen first enacted a law in 1970,[3] and the

[2]The research leading to these results has received funding from the European Union Seventh Framework Program (FP7/2007–2013) under grant agreement no. 608285—EUROPEAN INFORMATICS DATA EXCHANGE FRAMEWORK FOR COURTS AND EVIDENCE, http://www.evidenceproject.eu/. The views expressed in this chapter are solely the views of the authors, and do not necessarily reflect the views of the EVIDENCE consortium as a whole. The content of this chapter does not reflect the official opinion of the European Union. Responsibility for the information and views expressed therein lies entirely with the authors.

[3]Hessisches Datenschutzgesetz (1970), GVBl. 1970, 625.

Federal Republic gave itself a Code on Data Protection in 1977,[4] which has been continuously developed since. The Federal Constitutional Court first recognized the relevance of collecting and processing personal data for the free development of personality in its Micro-Census Decision of 1969,[5] and further developed this jurisprudence in its prominent Census Decision of 1983[6] leading to the recognition of a fundamental right to data protection derived from Article 1 (1) (human dignity) and Article 2 (freedom of personality) of the German Constitution (Grundgesetz, GG[7]).

Additionally, the privacy of telecommunications (and posts and correspondence) has been protected as a fundamental right by Article 10 of the German Constitution since the introduction of the constitution with the founding of the Federal Republic of Germany in 1949, and has continuously led to decisions of the Federal Constitutional Court since the first laws on surveillance were established in the late 1960s.

Data protection and privacy of telecommunications also politically and socially enjoy particular political and social attention and respect—it can be assumed that German history and the grave experiences of violations of these rights both in the Third Reich prior to 1945 and in the German Democratic Republic prior to 1989 have played an essential role in shaping the public's view on data protection and privacy of telecommunications, causing the related reflections both in the political and the legal system. As a result, Germany's laws are marked by a relatively well-defined system of checks and balances seeking to equate the recognized needs for threat-prevention and criminal investigation with adequate safeguards implemented into the underlying legal framework.

The German legal system is shaped by a fundamental distinction between two categories of measures that can be taken by LEAs, divided by their respective purpose: preventive and investigative measures. Preventive measures are measures taken to avert dangers and prevent threats—e.g., preventing a crime from happening or from continuing. Investigative measures are taken to investigate the crime (subsequently) and do not aim at preventing it (anymore), but at collecting the necessary evidence to allow for a trial against the potential offender.

2.2 *Preventive Measures*

The primary purpose of preventive measures is to intervene before an incident happens and thereby to prevent the harm, which would be caused by such incident.

---

[4]Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung (1977), BGBl. 1977, 201.

[5]BVerfG, Order of 16 July 1969—1 BvL 19/63—BVerfGE 27, 1.

[6]BVerfG, Judgment of the First Senate of 15 December 1983—1 BvR 209/83, 1 BvR 484/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83, 1 BvR 440/83—BVerfGE 65, 1.

[7]Basic Law for the Federal Republic of Germany, English version: http://www.gesetze-iminternet.de/englisch_gg/index.html. Accessed 26 September 2016.

Preventive measures are not limited to crime prevention,[8] which, however, forms a significant part of threat prevention. Preventive measures not only include actions aiming at the prevention of one particular event, but also include any action, which aims at terminating a dangerous status therefore, for example, the interruption of actions which as such consecutively (as opposed to isolated actions) constitute criminal offences. This is the case, for example, for deprivation of liberty in course of a kidnapping, in which the *continuous* deprivation of liberty constitutes a crime.

The major characteristic element of preventive measures is their intention to prevent harm from happening combined with the limited availability of prior knowledge, as well as with a simultaneous urge to counter-act as quickly as reasonably possible.

2.3 Investigative Measures

Investigative measures are measures intended to investigate a crime, hence to understand its background and to identify the acting offenders, and in particular to collect the necessary evidence. Investigative measures can be interrogation, seizure, arrest, lawful interception of telecommunications and several others. Investigative measures are typically taken subsequently to a crime, and thereby are distinct from preventive measures, which are taken prior to (or during) an (expected) crime. While methodologically the measures can be similar or identical on a technical level—e.g., lawful interception of telecommunications—the difference in purpose leads to different legal conditions and different authorities in charge. A measure can also be of a dual nature, hence serving both investigating a crime and preventing it from continuing (in case of consecutive crimes, which are not limited to one particular act, but e.g., to a continuous status such as "membership of a criminal organization").

The major characteristic element of investigative measures is their intention to understand a crime and to collect evidence for a subsequent trial. In contrast to preventive measures, the urge to act is usually reduced and so is the need to act under limited knowledge of the circumstances, so that the application of safeguards is easier. As a result, depending on the case, it may be possible to elaborate on the use of alternative less intrusive measures in the course of an investigation, which would not be possible under the pressing conditions of a preventive measure.

2.4 Resulting Legal Principles and Structures

This difference is reflected in the slightly less strict pre-conditions for preventive measures, taking into account the limited knowledge from the ex-ante view, the

[8]These measures also include all measures related to disaster prevention and readiness, crowd-management on sports events or political manifestations, or all sorts of minor illegitimate behaviour, which does not qualify as crime for being below the threshold of criminal activity (such as parking violations).

urge to act and the then still existing possibility to prevent the crime from actually happening (or at least terminating it). These facts influence the proportionality assessment in such a way that a preventive measure can still be proportionate under certain circumstances, where investigative measures would require higher safeguards and stricter procedural requirements.

2.5 *Considerations on Preventive Measures as a Scale for Investigative Measures*

Investigative measures need at a minimum the same safeguards as preventive measures and typically additional safeguards (or stricter conditions on exemptions, such as "case of urgency"). In that respect, the safeguards implemented into the law for preventive measures can serve as a scale for the absolute minimum requirements for investigative measures and as a starting point for further considerations. This is relevant for this chapter as the majority of innovative (and, usually, particularly intrusive) measures implemented into German law with regard to retrieving data from devices, systems and networks have been implemented as preventive measures only. The Code of Criminal Procedure, however, lacks codification of such measures, which has not prevented some German courts from reasoning that the existing provisions were sufficient to cover more intrusive measures, as well.[9] This is a rather questionable argument, however.

2.6 *German Police Forces, their Tasks and Corresponding Legal Framework*

Corresponding to the distinction outlined in the previous section and given the fact that Germany is a Federal State, the organization and legal framework of LEAs has a certain complexity. As a general rule, all measures for preventive purposes are governed by State law (German: Landesrecht) and executed by the States' police forces. There are basically three exceptions to this rule: border control (including airport and train security) is assigned to the Federal Police (German: Bundespolizei), tax and customs policing to Federal Customs Criminal Agency (German: Zollkriminalamt) and a few special tasks that need central coordination on federal level, such as specific preventive measures to counter international

[9]Landgericht Hamburg, Decision of 13 September 2010—608 Qs 17/10; Landgericht Landshut, 4 Qs 346/10.

terrorism, are assigned to the Federal Criminal Police Office (German: Bundeskriminalamt, BKA). All three are federal agencies and are governed by federal law accordingly.

The most relevant Code in the context of digital technologies is the Law on the Federal Criminal Police Office (German: Bundeskriminalamtgesetz,[10] BKAG), which since its promulgation in 2008 contains a chapter on preventive measures that can be taken by the Bundeskriminalamt to counter international terrorism. These include advanced technologies to infiltrate computer systems (computer-assisted search) or to intercept telecommunications prior to encryption by using hidden software on the system from which the data shall be intercepted.

Otherwise, preventive measures in the police sector are governed by the State police codes (e.g., Niedersächsisches Gesetz über die öffentliche Sicherheit und Ordnung)[11] and executed by the police forces of the States.

All investigative measures are governed by federal law: the German Code of Criminal Procedure (German: Strafprozessordnung, StPO).[12] Prosecution, however, is generally carried out by the prosecution agencies of the States, which are assisted by the state police forces, with the exception of certain categories of crime directed against the Federal Republic, such as offenses related to terrorism, for which the Federal Prosecution Office (German: Generalbundesanwalt) is in charge. The Federal Police, the Federal Customs Criminal Agency and the Federal Criminal Police Office can act to support prosecution offices additionally or in replacement of State police within the boundaries of their specific competences. In those cases, their respective codes apply (Bundespolizeigesetz,[13] Zollfahndungsdienstgesetz[14] and Bundeskriminalamtgesetz).[15]

[10]Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (Artikel 1 des Gesetzes über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten) (Bundeskriminalamtgesetz—BKAG); https://www.gesetze-im-Internet.de/bkag_1997/BJNR165010997.html. Accessed 10 January 2017.

[11]Niedersächsisches Gesetz über die öffentliche Sicherheit und Ordnung (Nds. SOG) in der Fassung, 19 January 2005. http://www.nds-voris.de/jportal/?quelle=jlink&query=SOG+ND+Inhaltsverzeichnis&psml=bsvorisprod.psml&max=true. Accessed 26 September 2016.

[12]Strafprozessordnung, English version: https://www.gesetze-im-Internet.de/englisch_stpo/englisch_stpo.html. Accessed 26 September 2016.

[13]Gesetz über die Bundespolizei (Bundespolizeigesetz—BPolG), https://www.gesetze-im-Internet.de/bgsg_1994/BJNR297900994.html. Accessed 26 September 2016.

[14]Gesetz über das Zollkriminalamt und die Zollfahndungsämter (Zollfahndungsdienstgesetz—ZFdG), https://www.gesetze-im-Internet.de/zfdg/BJNR320210002.html. Accessed 26 September 2016.

[15]S.a. FN 7.

3 Important Technical Developments and their Effects

3.1 Innovative Monitoring Technologies

The radical change in telecommunications technologies has likewise changed the technical framework for lawful interception, be it for preventive purposes or for investigative purposes. Packet-switched networks such as the Internet and accordingly voice over IP (VoIP) phone calls require different interception technologies than line-switched traditional networks. Traditionally, phone calls were intercepted by physically tapping the relevant subscriber line.

With the move of telephony into the digital domain and to packet-switched networks, telecommunications data is no longer distinct on a physical level (such as a single wire or a particular frequency), but only on a logical level (through address (meta) data). Correspondingly, the data stream containing the phone call, hence the respective protocols and the respective communication, needs to be identified within a much larger data stream, which is technically challenging and requires interception of large data quantities. As a result, lawful interception as carried out by LEAs are usually based on *legal obligations* of telecommunication service providers to route particular communications data streams requested in a warrant to the interception devices of a LEA.

There are exceptions, however, where technological advance prevents traditional techniques of interception from being effective. VoIP communications, for example, can easily be encrypted, rendering the content of communications inaccessible to the vast majority of agencies. For this reason, LEAs in Germany have acquired technologies to intercept VoIP calls on terminal devices of subscribers *prior to encryption*, rather than interception of the calls within transmission through networks. This, however, requires installing covert software intercepting the relevant data and routing it to the intercepting agency. Consequently, hidden access to the user's device needs to be established, and this kind of interception cannot be executed without altering data on that device.

For that reason, this kind of interception has been considered to be of genuine quality, and therefore needing to be based upon a specific legal base, providing for the necessary safeguards. Such a legal basis has been implemented into the Law on the Federal Criminal Police Office in § 20l BKAG for preventive measures with the specific purpose of countering international terrorism.

For investigative measures, however, no such legal basis exists in the German Code of Criminal Procedure (StPO), which is the reason why §100a StPO—the general allowance for lawful interception—is used in this context. In the light of the reasoning provided in Sect. 2.5 Considerations on Preventive Measures as a Scale for Investigative Measures, this is a practice raising questions as § 100a StPO does not provide for the same safeguards as § 20l BKAG, lacking, for example, an obligation to undo any alteration made to the infiltrated system.

3.2 Resulting New Quality of Impact on Fundamental Human Rights

Even more far-reaching is a practice referred to as a computer-assisted search. A computer-assisted search entails the covert and remote access to a particular device or system with the aim to extract data stored on it. Given the vast amounts of personal data stored on such devices and the comprehensive insights they allow into the personal life of the owner, such measures, have also been deemed to be of a totally new quality in comparison to existing methods. Additionally, as the data is not transferred (through a telecommunication network), rules on lawful interception (of telecommunications) do not apply for formal reasons. The Federal Constitutional Court of Germany has considered this category of measure to be intrusive in a different manner than lawful interception, and consequently derived a new fundamental right to integrity and confidentiality of IT systems that is considered to be potentially infringed by such measures (see Sect. 4.2.4).

4 Corresponding Judicature: Decisions of the Federal Constitutional Court and the Federal Supreme Court

4.1 The Federal Supreme Court's Decision on Computer-Assisted Search for Investigative Purposes

A first decision on computer-assisted search was issued by the German Supreme Court (German: Bundesgerichtshof, BGH) in early 2007.[16] It remains, at the time of writing, the only decision of a high court on *investigative* measures infiltrating IT systems.

The decision contains a couple of fundamental considerations. It has to be noted that this decision precedes the latter decisions of the Federal Constitutional Court establishing the fundamental right to integrity and confidentiality of IT systems, and does not yet reflect the particular considerations of the Federal Constitutional Court in that respect.

The Federal Supreme Court stated that a computer-assisted search was illegitimate for a lack of a legal basis, and in particular that such a measure could not be based upon the legal basis for search in the physical world (§ 102 StPO), as that provision did not allow for a covert search.[17] The idea of a search as codified in the

[16]BGH, Order of 31 January 2007—StB 18/06—BGHSt 51, 211, http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=pm&Datum=2007&Sort=3&anz=16&pos=0&nr=38779&linked=bes&Blank=1&file=dokument.pdf. Accessed 26 September 2016.

[17]BGH, Order of 31 January 2007—StB 18/06—headnote.

StPO related to an overt procedure of physical presence that was transparent in respect of the methods being used.[18]

A covert search was a more intrusive measure than an overt search,[19] which is why it could not be based on the general allowance for investigative measures laid down in § 161 StPO, which in addition can only generally be applied where no specific provisions on a particular measure exist and the impact on fundamental rights of the measure in question is minor.[20] Both conditions were not given in respect of a computer-assisted search.

Moreover, the Court held that a computer-assisted search aims at stored data, not data in transmission. As a result, § 100a StPO, i.e., the legal basis for lawful interception, could not apply.[21] It was illegitimate to combine elements of different legal bases allowing certain measure to create a legal basis for a genuine measure, not codified in the criminal procedure code.[22]

As a result of this ruling, computer-assisted searches have to be considered illegitimate for investigative purposes due to the lack of a legal basis in criminal procedure law. For preventive purposes, a legal basis for covert access to IT systems was codified in § 20k BKAG for measures taken by the BKA to counter international terrorism—a provision that has been subject to controversial discussion and to Federal Constitutional Court rulings, as the following sections will elaborate. The Supreme Court's decision has been fundamental in underpinning that innovative investigative measures cannot simply be based upon provisions which had been designed for measures in physical space (as opposed to online space) decades ago. In hindsight, this decision also needs to be seen in the light of the following decision of the Federal Constitutional Court establishing the fundamental right to integrity and confidentiality of IT systems and which has set additional requirements to the legal framework governing computer-assisted searches.

4.2 The Federal Constitutional Court's Decision on Computer-Assisted Search for Preventive Purposes

On 27 February 2008, the Federal Constitutional Court pronounced their decision[23] in the proceedings concerning two constitutional complaints, namely against § 5.2 no. 11 in conjunction with § 7.1, § 5 (3), § 5a (1) and § 1 of the North

[18]BGH, Order of 31 January 2007—StB 18/06—para. 5 with further references.

[19]BGH, Order of 31 January 2007—StB 18/06—para. 10.

[20]BGH, Order of 31 January 2007—StB 18/06—para. 21.

[21]BGH, Order of 31 January 2007—StB 18/06—para. 18.

[22]BGH, Order of 31 January 2007—StB 18/06—para. 22.

[23]BVerfG, Judgment of the First Senate of 27 February 2008—1 BvR 370/07—para. (1–333), http://www.bverfg.de/e/rs20080227_1bvr037007en.html. Accessed 26 September 2016.

Rhine-Westphalia Constitution Protection Act (VSG NRW),[24] and against § 5 (2) no. 11, § 5 (3), § 7 (2) and § 8 (4) sentence 2 in conjunction with §§ 10, 11 and § 17 (1) of the VSG NRW. These provisions regulated the powers of the Verfassungsschutz Nordrhein-Westfalen (North Rhine-Westphalian Office for the Protection of the Constitution) regarding various instances of data collection, in particular from IT systems, and the procedure for handling collected data. For instance, § 5 (2) no. 11 empowered the constitution protection authority to carry out two types of investigative measures: secret monitoring and other reconnaissance of the Internet, and secret access to IT systems. While secret monitoring was limited to obtaining knowledge of the contents of Internet communication only through the channel provided therefore, secret access to IT systems required the constitution protection authority to use technical infiltration in order to gain access to the system.

The appellants for the constitutional complaints claimed that the provisions were unconstitutional. The Federal Constitutional Court agreed and declared § 5 (2) no. 11 VSG NRW null and void, as the provision violated Article 2 (1) in conjunction with Article 1 (1), Article 10 (1) and Article 19 (1) sentence 2 GG. The decision was remarkable since the court claimed that there was an unwritten fundamental right to integrity and confidentiality of IT systems, which had not existed before, in order to react to the technological developments, i.e., the emerging use of IT systems in the daily life by a majority of citizens. The following sections will provide an overview on the different arguments considered by the Federal Constitutional Court with regard to the aforementioned alternatives, as well as the consequences arising from the judgment. The judgment distinguished between two constellations: "Secret Monitoring and Other Reconnaissance of the Internet" and "Secret Access to IT Systems."

4.2.1 Secret Monitoring and Other Reconnaissance of the Internet

According to the Federal Constitutional Court, the secret monitoring and reconnaissance of Internet communication (meaning any other techniques for Internet surveillance) as regulated in § 5 (2) no. 11 of VSG NRW violated the secrecy of telecommunication as guaranteed by Article 10 (1) GG, in which the fundamental right to telecommunication privacy is laid down. The scope of protection of Article 10 also covers telecommunication using IT systems connected to the Internet. However, it has to be noted that, according to a recent judgment,[25] the fundamental right aims at protecting the confidence that no third party obtains information about telecommunication, whereas the confidence of communication partners *in personam* is not protected. Consequently, investigative measures focusing on the

[24]The latest version of the VSG NRW is available at https://recht.nrw.de/lmi/owa/br_text_anzeigen?v_id=5520071121100436295. Accessed 26 September 2016.

[25]BVerfG, BVerfGE 106, 28 (37–38).

disappointment of the personal trust in the communication partner would not constitute a violation of Article 10, as opposed to accessing telecommunication without authorization. As a matter of fact, the question whether agencies are authorized to access telecommunication, is crucial for assessing whether measures are in violation of Article 10 GG.

With regard to communication via the Internet, the judgment contains several examples of different cases and their corresponding impact on Article 10 GG:

(i) If a state agency obtains knowledge of the contents of a telecommunication conducted via channels technically provided therefor without authorization, this constitutes a violation of Article 10 (1) GG[26];
(ii) The secret reconnaissance of the Internet communication also violates Article 10 (1) GG if the authority monitors secured communication contents by using access keys, which it collected without authorization or against the will of those involved in the communications[27];
(iii) In contrast to that, a violation of Article 10 (1) GG is to be denied if, for instance, a participant of a closed chatroom has voluntarily provided the authority with their access code[28];
(iv) In general, the state has the possibility to obtain publicly accessible information, e.g., by accessing communication contents that are available on the Internet addressing at least a group of individuals that is not further delimitated, e.g., accessing a website, subscribing to an open mailing list, monitoring a public chat room.[29]

According to the Federal Constitutional Court, the provisions as stipulated in § 5 (2) no. 11 VSG NRW, however, did not comply with the requirement of sufficiently clear provisions, as the preconditions for the corresponding measures are not sufficiently precise.[30] In addition, it was stated that the provision violated the principle of appropriateness, as it concerns not only suspicious persons, but also "communication partners"—and as a matter of fact, the broad wording of the preconditions would also allow the monitoring of persons who have not given cause for such measures.[31]

While the Federal Constitutional Court was rather clear when they declared the provision regarding secret monitoring and reconnaissance of Internet communication null and void, it was also stated that such measures are not denied to the authority under all circumstances.[32] In fact, measures for Internet reconnaissance would not cause any problems at all, as long as no fundamental rights are

[26]BVerfG, Judgment of the First Senate of 27 February 2008—1 BvR 370/07—para. 291.
[27]BVerfG, Judgment of the First Senate of 27 February 2008—1 BvR 370/07—para. 292.
[28]BVerfG, Judgment of the First Senate of 27 February 2008—1 BvR 370/07—para. 293.
[29]BVerfG, Judgment of the First Senate of 27 February 2008—1 BvR 370/07—para. 308.
[30]BVerfG, Judgment of the First Senate of 27 February 2008—1 BvR 370/07—para. 295.
[31]BVerfG, Judgment of the First Senate of 27 February 2008—1 BvR 370/07—para. 296, 297.
[32]BVerfG, Judgment of the First Senate of 27 February 2008—1 BvR 370/07—para. 302.

encroached. Provided that measures do not affect Article 10 GG as described above, a variety of other fundamental rights, however, need to be considered. According to the Federal Constitutional Court, the fundamental right to integrity and confidentiality of IT systems is not violated if the owner of data has opened their system technically to access data, e.g., by uploading content to a web server.[33] The right to informational self-determination is not affected as well, insofar as information obtained by the viewing public data is compiled, stored or evaluated using additional data, as this would cause a special danger for the personality of the affected individual.[34] Finally, the general right of personality is not affected, if information is already available on the Internet without any limitations with regard to the individuals being able to access data.[35]

In summary, it has to be noted that agencies are allowed to perform investigative measures such as Internet reconnaissance, as long as it is limited to information that is accessible for everybody. While the judgment declared provisions for investigative measures of constitutional protection authorities null and void, it can be also seen as an admission that measures such as collection of Open Source Intelligence can be lawful and even without any encroachments on fundamental rights.

4.2.2 Secret Access to IT Systems

The Federal Constitutional Court declared not only the provision allowing secret monitoring and reconnaissance of the Internet null and void, but also the provisions allowing the constitution protection authority to secretly access IT systems. Again, it was stated that this provision violated fundamental rights, in particular the general right of personality.[36] In addition, several fundamental principles had been violated, such as the principle of clarity of provisions, proportionality, and a lack of sufficient safeguards, i.e., precautions to protect the core area of private life.[37] Such precautions could be ensured with a two-tier concept. Firstly, the provision needs to ensure that collection of data of the core area of private life is avoided, as far as possible.[38] Secondly, if the relevance of data for the core area of private life cannot be ascertained before or during data collection, it has to be ensured that if data has been collected, the impact on the personality and development of the person concerned remains as low as possible.[39] In particular, any collected data should be

[33]BVerfG, Judgment of the First Senate of 27 February 2008—1 BvR 370/07—para. 306.

[34]BVerfG, Judgment of the First Senate of 27 February 2008—1 BvR 370/07—para. 307, 309.

[35]BVerfG, Judgment of the First Senate of 27 February 2008—1 BvR 370/07—para. 308.

[36]BVerfG, Judgment of the First Senate of 27 February 2008—1 BvR 370/07—para. 166.

[37]BVerfG, Judgment of the First Senate of 27 February 2008—1 BvR 370/07—para. 167.

[38]See on telecommunication surveillance BVerfG, BVerfGE 113, 348 (391–392); on acoustic monitoring of dwellings BVerfG, BVerfGE 109, 279 (318, 324).

[39]BVerfG, Judgment of the First Senate of 27 February 2008—1 BvR 370/07—para. 282.

screened and deleted without delay if it affects the core area of the subject's fundamental right.

As for the different fundamental rights concerned by secret access to IT systems, the Court stated that the secret access to IT systems can be used to perform a wide variety of different actions. If an individual's IT system is technically infiltrated in order to perform telecommunication surveillance, the impact of the infiltration goes far beyond the impact of conventional telecommunications surveillance, particularly since data which is not used for telecommunications could be accessed on the device.[40] Insofar as a measure serves to collect data from ongoing telecommunications (lawful interception on a terminal device, so-called Quellen-TKÜ), the violation is to be measured only against Article 10 GG.[41] In order to distinguish between the secret monitoring of the Internet as outlined above and secret access to an IT system through technical infiltration, the affected person needs to be able to take their own precautions against secret access.[42]

While the telecommunication itself is protected by Article 10 GG, this protection does not extend to information about or the content of telecommunications that are stored on a device (such as a complex IT system) after their completion.[43] This would, however, lead to a lack of protection if no other fundamental rights are applicable.

The guarantee of the inviolability of the home granted by Article 13 (1) GG guarantees an elementary space to the individual, in order to ensure a free development of an individual's personality. This leaves loopholes with regard to the access to IT systems. The scope of protection of Article 13 GG is the spatial sphere in which private life takes place.[44] While the protection is not restricted to the prevention of physical penetration—acoustic or optical monitoring of dwellings,[45] as well as the measurement of electromagnet radiation which could concern offline-systems[46] are within the scope of Article 13 GG. Article 13 does not offer protection for IT systems as such, regardless of the access modalities.[47] In addition, Article 13 does not apply to the collection of data by infiltrating an IT system, even if the system is located in a dwelling, as long as the dwelling itself remains untouched.[48]

Finally, the Federal Constitutional Court claimed that the right of personality, in particular in manifestation as the guarantees of the protection of privacy, and of the

[40]BVerfG, Judgment of the First Senate of 27 February 2008—1 BvR 370/07—para. 188.
[41]BVerfG, Judgment of the First Senate of 27 February 2008—1 BvR 370/07—para. 184.
[42]BVerfG, Judgment of the First Senate of 27 February 2008—1 BvR 370/07—para. 185.
[43]BVerfG, Judgment of the First Senate of 27 February 2008—1 BvR 370/07—para. 185.
[44]See BVerfG, BVerfGE 89, 1 (12); 103, 142 (150–151).
[45]See BVerfG, BVerfGE 109, 279 (309, 327).
[46]BVerfG, Judgment of the First Senate of 27 February 2008—1 BvR 370/07—para. 192.
[47]BVerfG, Judgment of the First Senate of 27 February 2008—1 BvR 370/07—para. 194.
[48]BVerfG, Judgment of the First Senate of 27 February 2008—1 BvR 370/07—para. 193, 195.

right to informational self-determination, did not comply sufficiently with the special need for protection of the user of IT-systems.[49]

As secret access to IT systems might not only reveal personal data, but also non-personal data, the right to privacy would not cover the integrity of the system as such.

The right to informational self-determination grants the individual the power to determine the disclosure and use of personal data.[50] It has to be considered that the use of IT systems might be required nowadays for an individual's personal development, making it inevitable to provide personal data to IT systems. At the same time, this creates the risk of data collection that can neither be detected nor prevented by the individual.[51] Third parties accessing such systems would be able to obtain vast amounts of personal data, which goes far beyond the impact of individual data collection against which the right to informational self-determination shall provide protection.[52] The right to informational self-determination therefore does not constitute a sufficient protection against the secret access to IT systems.

Overall, the secret access to IT systems was not covered by the scope of protection of any fundamental right existing at this point in time.

4.2.3 The New Fundamental Human Right to Integrity and Confidentiality of IT Systems

However, the Federal Constitutional Court acknowledged that there was a need to close this gap. In particular, there is a need to protect freedoms constituting significance for the personality.[53] The use of information technology is crucial for the personality and the development of the individual. However, the new possibilities offered by modern technologies (i.e., IT systems) could not have been predicted, while IT systems nowadays are omnipresent and their usage being central to the lives of many citizens. In 2007, one year before the judgment was pronounced, personal computers could be found in the large majority of households.[54] It also has to be noted that the performance of computers has increased, allowing the usage for a large number of different purposes, such as personal and business matters, a digital library or entertainment.[55] This applies even more in 2016, with recent developments regarding smart devices. IT systems therefore have a profound impact on daily life today, but also at the time of the judgment.

---

[49]BVerfG, Judgment of the First Senate of 27 February 2008—1 BvR 370/07—para. 196.

[50]See BVerfG, BVerfGE 65, 1 (43); 84, 192 (194).

[51]BVerfG, Judgment of the First Senate of 27 February 2008—1 BvR 370/07—para. 198–200.

[52]BVerfG, Judgment of the First Senate of 27 February 2008—1 BvR 370/07—para. 200.

[53]See BVerfG, BVerfGE 99, 185 (193); 114, 339 (346).

[54]See Federal Statistical Office (2007), p. 113.

[55]BVerfG, Judgment of the First Senate of 27 February 2008—1 BvR 370/07—para. 172.

Another development to be considered is the increase of networks in IT systems. In particular, the Internet as a complex combination of computer networks not only provides users with access to a mass of information to be retrieved from other network computers, but also with different services, e.g., for communication, allowing them to establish and maintain social contacts.[56] New risks have emerged as IT systems open up a broad spectrum of possible uses, many of them relying on the usage of personal data.[57] Additionally, a greater quantity of data has been produced compared to standalone systems.[58]

This data, however, could also be subject to manipulation or secret access.[59] Hidden collection or manipulation of personal data could also indirectly impair the freedoms of the citizen, as the fear of surveillance could have a chilling effect with regard to the usage of IT systems.[60] Consequently, there is a need for protection with regard to the significance of the use of information technology, on the one hand, and the emerging risks for fundamental rights as outlined above, on the other.[61] Consequently, there is a need for protection by fundamental rights to guarantee the confidentiality and integrity of information technology systems in order to ensure that the user's data, which is created, processed and stored by IT systems, is also protected.[62] According to the Federal Constitutional Court, such a fundamental right is a manifestation of the general right of personality. In order to properly consider all of the aforementioned technical developments, the judgment constituted a new fundamental right, namely the right to integrity and confidentiality of IT systems.

With regard to the subject of the proceedings, in particular the secret access to IT systems, the Federal Constitutional Court measured the constitutionality of the provisions against this new fundamental right. While it was acknowledged that secret access to IT systems was suitable to serve the purpose of threat prevention[63] and that there was no violation against the principle of necessity,[64] the Federal Constitutional Court deemed the measures to be a violation of the principle of appropriateness.[65] However, it was stated that such highly intrusive measures could meet the requirements of the principle of proportionality, if proper legal precautions were considered.[66]

---

[56]BVerfG, Judgment of the First Senate of 27 February 2008—1 BvR 370/07—para. 176.
[57]BVerfG, Judgment of the First Senate of 27 February 2008—1 BvR 370/07—para. 178.
[58]BVerfG, Judgment of the First Senate of 27 February 2008—1 BvR 370/07—para. 179.
[59]BVerfG, Judgment of the First Senate of 27 February 2008—1 BvR 370/07—para. 180.
[60]BVerfG, Judgment of the First Senate of 27 February 2008—1 BvR 370/07—para. 233.
[61]BVerfG, Judgment of the First Senate of 27 February 2008—1 BvR 370/07—para. 181.
[62]BVerfG, Judgment of the First Senate of 27 February 2008—1 BvR 370/07—para. 204.
[63]BVerfG, Judgment of the First Senate of 27 February 2008—1 BvR 370/07—para. 221.
[64]BVerfG, Judgment of the First Senate of 27 February 2008—1 BvR 370/07—para. 224.
[65]BVerfG, Judgment of the First Senate of 27 February 2008—1 BvR 370/07—para. 226.
[66]See BVerfG, Judgment of the First Senate of 27 February 2008—1 BvR 370/07—para. 247 et seq. for examples.

4.2.4 Comments on and Reactions to the Judgment

The judgment caused various reactions. It was claimed that the Federal Constitutional Court remained faithful to the line of judgments strengthening citizen's privacy with regard to investigative measures.[67] While the VSG-NRW could have been declared invalid due to the lack of protection for a core area of private life, it was acknowledged that the Federal Constitutional Court decided for a judgment establishing a principle, therefore reducing legal uncertainty for future legislation.[68] Establishing the right to integrity and confidentiality of IT systems was seen as a milestone, in particular due to the fact that the last judgment establishing a new fundamental right was the so-called "Volkszählungsurteil" in 1983, establishing the right to informational self-determination.[69] As a consequence, the judgment was seen as a preliminary end of the political debate regarding computer-assisted searches, allowing legislation to focus on the question on *how* a legal basis for such measures should be shaped.[70] Therefore, both parties involved claimed that the judgment was positive, even the unsuccessful party (the government of North Rhine-Westphalia), as the implementation of the judgment was seen as rather easy.[71] It also has to be acknowledged that the Federal Constitutional Court adjusted the legal reality to the technical reality by taking into account technological developments as well as the respective impact on the individual and society.

4.2.5 The Corresponding Changes to the Law on the Federal Criminal Police Office (BKAG)

In December 2008, shortly after the announcement of the presented Federal Constitutional Court's decision, the German Bundestag enacted a law[72] that amended the Law on the Federal Criminal Police Office (BKAG). This law assigned a new task to the Federal Criminal Police Office. According to the newly introduced § 4a BKAG, in certain situations and under certain circumstances,[73] in addition to conducting investigative measures, the BKA was authorized to carry out preventive surveillance measures in order to prevent dangers or risks posed by international terrorism. Until then, this task was principally assigned to the federal States

[67]Köpp et al. (2009), p. 43.

[68]Kudlich (2008), p. 478.

[69]Tschentscher (2008), p. 383.

[70]Bär (2008), p. 325.

[71]Schramm and Jansen (2008), p. 6.

[72]Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt of 25 December 2008 (BGBl.I, 3083), http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl108s3083.pdf. Accessed 23 September 2016.

[73]These circumstances are elaborated further in the provision.

(German: Bundesländer). In other words, § 4a BKAG enabled the Federal Criminal Police Office to act preventively as well. In addition to that, the aforementioned law introduced a new subsection to the BKAG.[74] This subsection consists of §§ 20a–20x, vesting the BKA with different powers to fulfill the task introduced in § 4a, some of them aiming at the collection of electronic evidence and allowing the use of innovative monitoring techniques (see above Sect. 3.1).

Of particular interest here is § 20k BKAG, allowing the BKA to covertly access IT systems (computer-assisted searches). The wording of this provision closely adhered to the requirements established by the BVerfG in its judgment on the computer-assisted search for preventive purposes (see above), adopting the reasoning of the court word-for-word when formulating the legal prerequisites for carrying out such a measure.[75] Likewise, these amendments (like amendments to other laws in the field of security) were supposed to respond to technical developments, in particular to the increased significance of IT systems, taking into account that they are used for criminal and terrorist purposes as well.[76]

4.3 *The Federal Constitutional Court's Decision on the Law on the Federal Criminal Police Office (Preventive Measures)*

The rules and powers laid down in §§ 20a–20x BKAG have been very controversial, both in terms of their practical utility and in terms of the legal aspects. The main sources of legal controversy have concerned their constitutionality in the light of the Federal Constitutional Court's decision of 2008, and regarding the question whether the BKA may have executive powers at all.[77] Allowing direct and hidden access to a person's terminal device e.g., the personal computer, and collecting data from the device (German term for the measure: Online-Durchsuchung), § 20k BKAG has been considered the most intensely discussed provision of the whole BKAG.[78]

[74]Subsection 3a: „Abwehr von Gefahren des internationalen Terrorismus" (The Protection Against Threats from International Terrorism).

[75]Bundesministerium des Innern and Bundesministerium der Justiz (2013), p. 26.

[76]Bundesministerium des Innern and Bundesministerium der Justiz (2013), pp. 8 et seq.

[77]Kugelmann (2014), § 1 para. 5 et seq.

[78]Kugelmann (2014), § 20 k para. 1 et seq.

After the amendment, a number of constitutional complaints were filed against the aforementioned, newly inserted provisions of the BKAG. The First Senate of the Federal Constitutional Court combined these complaints into one proceeding and rendered its judgment on the constitutionality of the impugned provisions on 20 April 2016.[79]

The complainants had impugned several provisions and claimed violation of various fundamental rights guaranteed by the German Constitution.[80] The Federal Constitutional Court, above all, decided on the compliance of the impugned BKAG-provisions with:

(i) The fundamental right to informational self-determination;
(ii) The fundamental right to the integrity and confidentiality of IT systems;
(iii) The fundamental right to the inviolability of the home, and;
(iv) The fundamental right to secrecy of telecommunication.

4.3.1 Constitutional Requirements for Carrying Out Surveillance Measures

With the judgment of the First Senate of 20 April 2016, the Federal Constitutional Court, first of all, decided that the specific regulation of the investigating powers in many regards does not fulfill the requirements of the principle of proportionality.[81]

Whereas the challenged provisions of the BKAG serve the legitimate purpose to provide the BKA with investigative measures in order to fulfill the task to protect against threats of international terrorism, and comply with the requirements of suitability and necessity,[82] the BVerfG decided that in several aspects they lack the last element of proportionality, namely *reasonableness* (in Germany also referred to as "proportionality in the narrower sense," Verhältnismäßigkeit im engeren Sinne).[83]

Since the challenged powers of the BKA authorize serious interference with privacy and thus affect fundamental rights, they have to fulfill the following criteria:

---

[79]BVerfG, Judgment of the First Senate of 20 April 2016—1 BvR 966/09—1 BvR 1140/09—http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2016/04/rs20160420_1bvr096609.html. Accessed 23 September 2016.

[80]Article 2 (1) in conjunction with Article 1 (1), Article 3 (1), Article 5 (1) sentence 2, Article 10, Article 12, and Article 13, partially in conjunction with Article 1 (1), Article 19 (4), and Article 20 (3) GG; See BVerfG, Judgment of the First Senate of 20 April 2016—1 BvR 966/09—1 BvR 1140/09—para. 2 et seq., 5.

[81]See BVerfGE 67, 157 (173); 70, 278 (286); 104, 337 (347 ff.); 120, 274 (318 f.); 125, 260 (316); constant jurisdiction.

[82]BVerfG, Judgment of the First Senate of 20 April 2016—1 BvR 966/09—1 BvR 1140/09—para. 96 et seq.

[83]See BVerfG, Judgment of the First Senate of 20 April 2016—1 BvR 966/09—1 BvR 1140/09—para. 145 et seq.

(i) To be limited to the protection or reinforcement of a substantial legally protected right, good or interest;
(ii) To presuppose a precisely foreseeable threat posed to these rights, goods or interests;
(iii) To extend to third persons in the surroundings of the responsible person only under certain and limited circumstances;
(iv) In most cases, to provide specific regulation and precautions in order to protect the core area of private life and the persons whose profession swears them to confidentiality;
(v) To guarantee transparency, individual legal relief and judicial review, and supervisory control;
(vi) To be flanked by duties to delete the data collected.[84]

In addition to that, the provisions authorizing the BKA to carry out surveillance measures must generally comply with the principle of clarity and definiteness of legal provisions,[85] which serves the purposes to enable the citizens to foresee possible interference with their rights, to limit the authorities' powers, and to enable effective judicial control.[86] Because of their deep intrusion into the private sphere of the persons subjected to these measures, who because of their covertness at the same time in most cases will not be able to proceed against these measures, this principle, according to the BVerfG, must be handled very strictly with regard to the challenged powers of the BKA.[87]

4.3.2 The Constitutionality of § 20k BKAG (Covert Access to IT Systems)

Together with the surveillance of private homes, the access to IT systems is considered to interfere with privacy in the most serious and grave way possible.[88] The Court's decision on the constitutionality of the BKA's authorization to do so in § 20k BKAG therefore deserves closer examination.

The Federal Constitutional Court decided that the provision authorizing the BKA to access IT systems did not completely meet the aforementioned requirements. It ruled that § 20k BKAG, among others, is not compliant with the

[84]See BVerfG, Judgment of the First Senate of 20 April 2016—1 BvR 966/09—1 BvR 1140/09—headnote 1.b), para. 103–144: 104–108, 109–113, 114–116, 117–118, 119–129, 131–133, 134–143, 144.

[85]BVerfG, Judgment of the First Senate of 20 April 2016—1 BvR 966/09—1 BvR 1140/09—para. 94.

[86]See BVerfG, BVerfGE 113, 348 (375 ff.); 120, 378 (407 f.); 133, 277 (336 para. 140); constant jurisdiction.

[87]BVerfG, Judgment of the First Senate of 20 April 2016—1 BvR 966/09—1 BvR 1140/09—para. 94.

[88]BVerfG, Judgment of the First Senate of 20 April 2016—1 BvR 966/09—1 BvR 1140/09—para. 105.

fundamental rights to informational self-determination[89] and to secrecy of telecommunication,[90] and hence ruled it unconstitutional.[91] However, the BVerfG did not declare the provision null and void, but decided that it has to be revised by no later than 30 June 2018. Until that date, the current provision remains in force, but has to be applied in conformity with the constitution as outlined in the considerations of the Federal Constitutional Court in the judgment of 20 April 2016.[92]

As regards the legal prerequisites for carrying out the measure, the BVerfG decided that § 20k BKAG can be interpreted in conformity with the constitution, but also that it is unconstitutional with regard to the precautions included in order to protect the core area of private life.[93]

The measure interferes with the right to integrity and confidentiality of IT systems,[94] which implicates severe requirements especially regarding the sufficient foreseeability of a specific danger of terroristic criminal acts.[95] In this respect, the BVerfG, in particular, criticizes one particular sentence of the provision,[96] and stated that with regard to this sentence, the German constitution requires a narrowed interpretation.[97]

In addition to that, the Federal Constitutional Court applied the fundamental right to confidentiality and integrity of IT system's requirements for access to IT systems, developed in its decision of 27 February 2008 (see Sect. 4.2), to § 20k BKAG in order to assess its precautions for the protection of the core area of private life.[98] The court ruled that the BKAG provision does not meet those constitutional requirements completely,[99] as far as downstream precautions for the protection of the core area are concerned.[100] According to § 20k (7) sentences 3 and 4 BKAG, data collected through access to IT systems must be screened for possible content with relevance to

[89]Article 2 (1) in conjunction with Article 1 (1) GG.

[90]Article 10 (1) GG.

[91]See BVerfG, Judgment of the First Senate of 20 April 2016—1 BvR 966/09—1 BvR 1140/09—operative provision 3.

[92]BVerfG, Judgment of the First Senate of 20 April 2016—1 BvR 966/09—1 BvR 1140/09—operative provision 4.

[93]BVerfG, Judgment of the First Senate of 20 April 2016—1 BvR 966/09—1 BvR 1140/09—para. 208, 217 et seq.

[94]BVerfG, Judgment of the First Senate of 20 April 2016—1 BvR 966/09—1 BvR 1140/09—para. 209 et seq.

[95]BVerfG, Judgment of the First Senate of 20 April 2016—1 BvR 966/09—1 BvR 1140/09—para. 212.

[96]§ 20k (1) sentence 2 BKAG.

[97]BVerfG, Judgment of the First Senate of 20 April 2016—1 BvR 966/09—1 BvR 1140/09—para. 213.

[98]BVerfG, Judgment of the First Senate of 20 April 2016—1 BvR 966/09—1 BvR 1140/09—para. 217–220.

[99]BVerfG, Judgment of the First Senate of 20 April 2016—1 BvR 966/09—1 BvR 1140/09—para. 221.

[100]BVerfG, Judgment of the First Senate of 20 April 2016—1 BvR 966/09—1 BvR 1140/09—para. 223 et seq.

the core area of private life. As stated by the BVerfG, the body tasked with this inspection of the collected data must be sufficiently independent from the BKA, which means that external persons not involved in security tasks should be the ones actually carrying out the task and such persons independent from the BKA must be responsible for the decision-making.[101] According to § 20k (7) sentences 3 and 4 BKAG, on the contrary, the screening of the collected data lies only in the hands of personnel from the Federal Criminal Police Office. The BVerfG decided that whereas it is still possible to involve employees of the BKA additionally for investigation-specific and technical support, it is not sufficient to make recourse to the Office's Data Protection Officer to carry out the screening, even if they are free from directives as it is the case according to the challenged provision of the BKAG.[102]

Moreover, the Federal Constitutional Court objected to the storage duration of protocols documenting the deletion of data.[103] Laid down in § 20k (7) sentence 8 BKAG is the duty to store these protocols until the end of the year following the year of the documentation at the longest. According to the BVerfG, this does not meet the constitutional requirement to protocol the deletion in a way that allows an eventual (subsequent) control.[104]

4.3.3 Other Important Aspects of the Judgment with Regard to Electronic Evidence

The judgment of the First Senate of 20 April 2016 includes considerations regarding other impugned provisions authorizing the BKA to carry out investigative measures relevant in this context.

The design of the legal prerequisites in § 20j BKAG, allowing electronic profile searching (German: Rasterfahndung) and interfering with the fundamental right to informational self-determination, is constitutional,[105] being sufficiently specific and proportionate and requiring a concrete threat and a judicial order.[106]

In contrast, the provision dealing with the lawful interception of on-going telecommunication (§ 20l BKAG, German terms: Telekommunikationsüberwachung/TKÜ, and Quellen-TKÜ), interfering with the fundamental right to secrecy of telecommunication—

[101]BVerfG, Judgment of the First Senate of 20 April 2016—1 BvR 966/09—1 BvR 1140/09—para. 224.

[102]BVerfG, Judgment of the First Senate of 20 April 2016—1 BvR 966/09—1 BvR 1140/09—para. 224 et seq.

[103]BVerfG, Judgment of the First Senate of 20 April 2016—1 BvR 966/09—1 BvR 1140/09—para. 226.

[104]BVerfG, Judgment of the First Senate of 20 April 2016—1 BvR 966/09—1 BvR 1140/09—para. 129, 226; See BVerfGE 109, 279 (318 f., 332 f.); 113, 348 (392); 120, 274 (337, 339).

[105]BVerfG, Judgment of the First Senate of 20 April 2016—1 BvR 966/09—1 BvR 1140/09—para. 206.

[106]BVerfG, Judgment of the First Senate of 20 April 2016—1 BvR 966/09—1 BvR 1140/09—para. 207.

not with the right to confidentiality and integrity of IT systems[107]—only partially complies with the fundamental rights guaranteed by the German constitution. On the one hand, the part of the provision that extends the scope of such surveillance to the prevention of criminal offences (§ 20l (1) no. 1–4 BKAG) is too unspecific and disproportionately broad and therefore unconstitutional.[108] On the other hand, however, the additional requirements for subsidiary lawful interception through direct access to a terminal device (Quellen-TKÜ) laid down in § 20l (2) BKAG are sufficient.[109] Also, as with § 20k BKAG, the storage period for protocols about the deletion of data was held to be too short and thus unconstitutional.[110]

In general, with the judgment of 20 April 2016, the BVerfG ruled that all investigative and surveillance powers challenged by the complainants lack supplementary provisions in order to be proportional (see Sect. 4.3.2 above).[111]

In addition, the judgment addressed the further use of data collected (i.e., extending beyond the original investigation procedure), the transfer of data to other German authorities for other purposes, and finally, the requirements for the transfer of data to authorities in third countries, deciding on the latter for the first time.[112] These issues concern the use, rather than the collection, of electronic evidence, so these parts of the decision will not be presented in detail here.

To sum up, with this judgment, the Federal Constitutional Court has consolidated constitutional case law of the past years with respect to:

(i) Legal requirements for covert surveillance measures, and;
(ii) The transfer of data to third-party authorities for other purposes.[113]

4.3.4 The Lack of Unanimity of the Decision and Reactions

The First Senate of the Federal Constitutional Court did not adopt the judgment unanimously. Three out of eight judges voted against it,[114] two of whom delivered

[107]BVerfG, Judgment of the First Senate of 20 April 2016—1 BvR 966/09—1 BvR 1140/09—para. 228.
[108]BVerfG, Judgment of the First Senate of 20 April 2016—1 BvR 966/09—1 BvR 1140/09—para. 232.
[109]BVerfG, Judgment of the First Senate of 20 April 2016—1 BvR 966/09—1 BvR 1140/09—para. 234.
[110]BVerfG, Judgment of the First Senate of 20 April 2016—1 BvR 966/09—1 BvR 1140/09—para. 246.
[111]BVerfG, Judgment of the First Senate of 20 April 2016—1 BvR 966/09—1 BvR 1140/09—para. 253 et seq.
[112]BVerfG, Judgment of the First Senate of 20 April 2016—1 BvR 966/09—1 BvR 1140/09—para. 275 et seq.
[113]Federal Constitutional Court (2016), Press Release no. 19/2016.
[114]BVerfG, Judgment of the First Senate of 20 April 2016—1 BvR 966/09—1 BvR 1140/09—para. 359.

separate opinions, explaining why and in what respects they did not back the judgment and its key considerations. These separate opinions are attached to the judgment.[115] According to the separate opinions, an interpretation of most of the challenged provisions in conformity with the constitution would be possible and sufficient. One of the judges considered the requirements set by the First Senate as too strict and detailed,[116] and the other pointed to the fact that measures must be reasonably practicable.[117]

The judgment of the majority of the judges of the First Senate caused varied reactions. There have been critical comments claiming that the Court has gone too far, thus sympathizing with the separate opinions[118] or stating that it arrogates detailed knowledge in criminal investigations and setting scrupulously precise requirements.[119] Others have been more appreciative of the judgment, in particular regarding its requirements for the protection of persons whose profession swears them to confidentiality, e.g., lawyers,[120] or in general stating that the decision was pointing the way ahead for the legislator, the German security architecture and for the self-conception of a free and democratic state under the rule of law.[121]

5 Conclusion

5.1 Considerations on Investigative Measures to Be Drawn from These Developments

The development and use of new telecommunications technologies, in particular packet-switched networks (such as the Internet) have led to fundamental changes in techniques to lawfully intercept telecommunications in Germany. In particular, rather than intercepting encrypted telecommunications in transmission, methods to route telecommunications content data directly from terminal devices to interception equipment prior to encryption by using covert software, have been adopted. Additionally, the availability of large quantities of personal data on personal devices have led to the establishment of computer-assisted searches—the covert access to data on such devices by secretly implemented software (technically

[115]Separate opinions to Judgment of the First Senate of 20 April 2016—1 BvR 966/09—1 BvR 1140/09: Eichberger (para. 1–16) and Schluckebier (para. 1–29).

[116]Separate opinion to Judgment of the First Senate of 20 April 2016—1 BvR 966/09—1 BvR 1140/09—Eichberger, para. 7.

[117]Separate opinion to Judgment of the First Senate of 20 April 2016—1 BvR 966/09—1 BvR 1140/09—Schluckebier, para. 16.

[118]Sachs (2016), p. 664.

[119]Wiemers (2016), p. 840.

[120]Lührig (2016).

[121]Buchholz (2016), p. 906.

comparable to Trojan horse software). The specific intrusiveness of such measures, specifically their impact on fundamental rights, have been reflected in the jurisdiction of the German Federal Constitutional Court.

With the development of the new fundamental right to integrity and confidentiality of IT systems in the judgment of 27 February 2008, the Federal Constitutional Court has stayed abreast of changes by adapting constitutional guarantees to recent developments in technology, society and law enforcement. As provisions assigning investigative powers to LEAs and actions based upon them have to be measured against this fundamental right too, this decision is also meaningful for criminal investigation proceedings. However, it has to be noted that the Federal Constitutional Court also stated that secret monitoring and other reconnaissance of the Internet is not, in principle, denied to authorities. In particular, the state may obtain publicly accessible information, e.g., by accessing communication contents that are available on the Internet addressing all readers or at least a group of individuals that is not further delimitated. In fact, neither the fundamental right to telecommunication's privacy nor the right to integrity and confidentiality of IT systems, the right to informational self-determination or the general right of personality is affected by measures related to publicly available data. While the judgment established a new fundamental right in order to protect citizen's privacy, it also outlined the constitutional requirements for Open Source Intelligence measures.

In December 2008, a new task in the field of prevention was assigned to the Federal Criminal Police Office and several investigative powers in this field were introduced in the BKAG in order to fulfill this new task. This amendment rearranged the distribution of responsibilities between the Federal State (Bund) and its States (Länder), because the BKA is a central agency on the federal level. With the judgment of 16 April 2016 on the constitutionality of these new BKAG-provisions, the Federal Constitutional Court has countered the expansion of such investigative powers through laws or their extensive application. This was the case in a number of other decisions rendered by the Federal Constitutional Court since 2011.[122] In the judgment of 16 April 2016, essential requirements for covert surveillance measures have been developed, which are formulated in a way that permits transfer of their principles to surveillance measures carried out when investigating crimes after they have already been committed. Investigative powers have to respect the fundamental rights guaranteed by the German constitution as well. As described above Sect. 2.4, because of the different purpose and perspective, they rather have to follow stricter rules than preventive measures. Thus, this judgment is of great relevance for covert surveillance measures in general.

[122]See, e.g., BVerfG, Order of 4 April 2006—1 BvR 518/02—BVerfGE 115, 320; Judgment of 11 March 2008—1 BvR 2074/05, 1 BvR 1254/07—BVerfGE 120, 378; Judgment of 2 March 2010–1 BvR 256/08—et al., BVerfGE 125, 260; Judgment of 24 April 2013—1 BvR 1215/07—BVerfGE 133, 277.

Still, while the legislative framework has undergone several amendments to meet the requirements of the aforementioned constitutional court's decision, these amendments have been limited to the governance of preventive measures, and mostly to those being taken by BKA. The legal framework for investigative measures has only seen minor changes, such as the introduction of § 100i StPO governing the use of IMSI catchers. The use of covert software to intercept telecommunications prior to encryption, however, remains unregulated in the Code of Criminal Procedure, albeit the strict requirements laid down for preventive measures in § 20l BKAG a fortiori should apply on investigative measures of the same nature, as well. Only regarding computer-assisted search, the German Supreme Court has ruled in 2007 that it cannot be based upon the existing legal bases for the lack of adequate safeguards.

5.2 Outlook

Surveillance measures and the related legal framework remain a controversial topic in Germany. Still, the focus seems to lie on the new competences of BKA in the field of preventive measures, the data retention debate and—since the Snowden revelations in 2013—particularly on the competences of the various German Intelligence Agencies. While investigative measures had briefly been in focus subsequently to the mentioned Supreme Court's decision in 2007, the discussion seems to have ebbed off ever since. This is unfortunate, as investigative measures according to the German laws' fundamental principles require equal or higher safeguards than preventive measures, and that lack of legal governance of intercepting telecommunications prior to encryption through covert software secretly installed on a device should, in the view of the authors, not be based upon the existing (traditional) legal rules on lawful interception, which were designed once for (physical) wire-tapping of telephone lines. Rather the specific safeguards laid down for such measures for preventive purposes in § 20l BKAG, such as the requirement to automatically undo alterations imposed upon the infiltrated system, should be codified for investigative measures as well. However, currently[123] there are no signs that the legislator would wish to take any steps to amend the corresponding legal framework for investigative measures—the German Code of Criminal Procedure.

Acknowledgements We would like to thank Lisa Schulz for supporting us in the research for this chapter.

[123] August 2016.

References

Bär W (2008) BVerfG: Verfassungsmäßigkeit der Online-Durchsuchung und anderer verdeckter Ermittlungsmaßnahmen in Datennetzen. MMR 5:315–327

Buchholz G (2016) Kein Sonderopfer für die Sicherheit. BVerfG erklärt BKAG für verfassungswidrig. NVwZ 13:906–909

Bundesministerium des Innern and Bundesministerium der Justiz (2013) Bericht der Regierungskommission zur Überprüfung der Sicherheitsgesetzgebung in Deutschland, http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2013/regierungskommission-sicherheitsgesetzgebung.pdf;jsessionid=0A82D2A7A0445A4E0C02956395DEF2C8.2_cid295?__blob=publicationFile. Accessed 23 Sept 2016

Federal Constitutional Court (2016) Press release no. 19/2016, 20 April 2016, https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2016/bvg16-019.html. Accessed 23 Sept 2016

Federal Statistical Office (2007) Statistisches Jahrbuch 2007 Für die Bundesrepublik Deutschland/Statistical Yearbook 2007 For the Federal Republic of Germany. Wiesbaden, https://www.destatis.de/DE/Publikationen/StatistischesJahrbuch/Jahrbuch2007.pdf?__blob=publicationFile. Accessed 23 Sept 2016

Köpp L, Kowalzik S, Recktenwald B (2009) BVerfG v. 27.2.2008 — 1 BvR 370/07 u. 1 BvR 595/07. RubRR 2:36–46

Kudlich H (2008) Enge Fesseln für „Landes- und Bundestrojaner" – Anforderungen an die Zulässigkeit einer (sicherheitsrechtlichen) Online-Durchsuchung. JA 6:475–478

Kugelmann D (2014) BKA-Gesetz. Nomos, Baden-Baden

Lührig N (2016) BKA-Gesetz: Schutzkonzept für Anwälte vor heimlicher Überwachung verfassungswidrig, 20 April 2016. https://anwaltsblatt.anwaltverein.de/de/rechtsprechung/bka-gesetz-schutzkonzept-von-anwaelten-vor-heimlicher-ueberwachung-verfassungswidrig. Accessed 23 Sept 2016

Sachs M (2016) Grundrechte: Heimliche Überwachungsmaßnahmen. Nur grundsätzliche Verfassungsmäßigkeit der Ermächtigung des BKA zum Einsatz von heimlichen Überwachungsmaßnahmen zur Terrorismusabwehr. JuS 7:662–664

Schramm M, Jansen K (2008) Die Online-Durchsuchung im Lichte der Rechtsprechung. Jur. Info 1:1–7

Tschentscher A (2008) Das Grundrecht auf Computerschutz. AJP/PJA 4:383–393

Wiemers M (2016) Teilweise Verfassungswidrigkeit des BKA-Gesetzes. NVwZ 12:839–841

LegalAIze: Tackling the Normative Challenges of Artificial Intelligence and Robotics Through the Secondary Rules of Law

Ugo Pagallo

Abstract A considerable number of studies have been devoted over the past years, to stress risks, threats and challenges brought on by the breath-taking advancements of technology in the fields of artificial intelligence (AI), and robotics. The intent of this chapter is to address this set of risks, threats, and challenges, from a threefold legal perspective. First, the focus is on the aim of the law to govern the process of technological innovation, and the different ways or techniques to attain that aim. Second, attention is drawn to matters of legal responsibility, especially in the civilian sector, by taking into account methods of accident control that either cut back on the scale of the activity via, e.g., strict liability rules, or aim to prevent such activities through the precautionary principle. Third, the focus here is on the risk of legislation that may hinder research in AI and robotics. Since there are several applications that can provide services useful to the well-being of humans, the aim should be to prevent this threat of legislators making individuals think twice before using or producing AI and robots. The overall idea is to flesh out specific secondary legal rules that should allow us to understand what kind of primary legal rules we may need. More particularly, the creation of legally de-regulated, or special, zones for AI and robotics appears a smart way to overcome current deadlocks of the law and to further theoretical frameworks with which we should better appreciate the space of potential systems that avoid undesirable behavior.

Keywords Accident control · Artificial intelligence · Liability · Robotics · Secondary rules

U. Pagallo (✉)
Giurisprudenza, Università di Torino, Turin, Italy
e-mail: ugo.pagallo@unito.it

M. Corrales et al. (eds.), *New Technology, Big Data and the Law*,
Perspectives in Law, Business and Innovation, DOI 10.1007/978-981-10-5038-1_11

Contents

1 Introduction

A considerable number of studies have been devoted over recent years, to stress risks, threats and challenges brought on by the breath-taking advancements of technology in the fields of artificial intelligence (AI), and robotics. In November 2012, a non-profit US based NGO, Human Rights Watch, released a document, *Losing Humanity*, proposing a ban on "killer robots," namely "fully autonomous weapons that could select and engage targets without human intervention." In 2015, another NGO, the Future of Life Institute, presented an open letter addressing the challenges triggered by AI and robotics: "Its members—and advocates, among which Bill Gates, Elon Musk, and Stephen Hawking—are concerned that as increasingly sophisticated achievements in AI accumulate—especially where they intersect with advances in autonomous robotics technology—not enough attention is being paid to safety." Whilst the White House Office of Science and Technology Policy has conducted a series of public workshops on questions of AI and policy in 2016, an Industry Connections Program within the IEEE Standards Association, namely The Global Initiative for Ethical Considerations in the Design of Autonomous Systems, is currently drafting another document that addresses "ethical concerns for autonomous and intelligent systems design." Although this latter document is still in progress, attention should be drawn to the eight sectors under scrutiny: (i) personal data and privacy control; (ii) the law of autonomous and intelligent systems; (iii) safety and beneficence of artificial general intelligence and super-intelligence; (iv) economics of machine automation and humanitarian issues; (v) methodologies to guide ethical research, design, and manufacturing; (vi) methodologies to imbue ethics and values into AI; (vii) lethal autonomous weapons systems; and, (viii) general principles that apply to all types of autonomous and intelligent systems regardless of whether they are physical robots, e.g., care robots or driverless cars, or software AI systems.

Against this framework, we should reflect on a crucial point, in order to properly appreciate current analyses and documents on the normative challenges of AI and robotics. From a technical point of view, an increasing number of robots, such as AI domestic assistants, robo-traders and robo-warriors, home security and surveillance applications, are not a mere "out of the box" machine. Rather, these machines can

"sense," "think," and "act," at least in the engineering meaning of these words.[1] Robots and further artificial agents (AA) can respond to stimuli by changing the values of their properties or inner states and furthermore, they can improve the rules through which those properties change without external stimuli.

As a sort of prolonged epigenetic developmental process, this means that AAs progressively gain knowledge or skills from their own interaction with the living beings inhabiting the surrounding environment and hence, more complex cognitive structures emerge in the state-transition system of the AA. Specimens of the same model will behave in quite different ways, according to the complexity of the context and how humans train, treat, or manage them. Whilst the behavior and decisions of these AAs can be unpredictable and risky, their conduct also affects traditional notions of the law and of ethics, such as matters of foreseeability and reasonability, negligence and due care. All in all, this is going to be the first time ever that humans will be held accountable for what an artificial state-transition system "decides" to do. Although current legal systems conceive such machines as simple means of human interaction, we should consider some of them as proper "agents." Therefore, how should legal systems deal with the peculiar unpredictability and risky behavior of robots and smart AI systems? How can we program these machines, and instruct them so as to tell what is "right" and what is "wrong" about their own conduct? Should we privilege the outcomes of AI and robotic behavior, or judge the latter vis-à-vis the intent behind such actions? Or, some mix of both of them?

The intent of this chapter is to address the normative challenges of AI and robotics from a threefold legal perspective. Section 2 dwells on the aim of the law to govern the process of technological innovation, and the different ways or techniques to attain that aim. Section 3 deepens this analysis in terms of legal responsibility, especially in the civilian sector, by taking into account methods of accident control that either cut back on the scale of the activity via, e.g., strict liability rules, or aim to prevent such activities through the precautionary principle. The result is legislations that may hinder the research in AI and robotics. Since we are talking about several applications that, in the words of the UN World Robotics report, can provide "services useful to the well-being of humans,"[2] Sect. 4 examines how to prevent this threat of lawmakers making individuals think twice before using or producing AI and robots.

The overall idea is to define a set of specific secondary legal rules that would allow us to understand what kind of primary legal rules we may need. More particularly, the creation of legally de-regulated, or special, zones for AI and robotics appears a smart way to overcome current deadlocks of the law and to further theoretical frameworks with which we should better appreciate the space of

[1]Suffice it to mention work of Wooldridge and Jennings (1995), Franklin and Graesser (1997), Allen et al. (2000), and Floridi and Sanders (2004).

[2]See UN (2005).

potential systems that avoid undesirable behaviors. Although reasonable compromises are, at times, necessary in the legal field, its secondary rules may help us to discover the right answer.

2 The Goals of the Law

The aim of the law to govern the race of technological innovation comprises different purposes and ways in which human and artificial behavior can be regulated.[3] Some suggest that we should distinguish four main legislative goals, such as: (a) the achievement of particular effects; (b) functional equivalence between online and offline activities; (c) non-discrimination between technologies with equivalent effects; and, (d) future-proofing of the law that should neither hinder the advance of technology, nor require over-frequent revision to tackle such a progress.[4] Others propose to differentiate between (a) technological indifference, i.e., legal regulations which apply in identical ways, whatever the technology, as occurs with the right to authorize communication of a work to the public in the field of copyright law; (b) implementation neutrality, according to which regulations are by definition specific to that technology and yet, they do not favor one or more of its possible implementations, e.g., the signature of e-documents; and, (c) potential neutrality of the law that sets up a particular attribute of a technology, although lawmakers can draft the legal requirement in such a way that even non-compliant implementations can be modified to become compliant.[5]

As to the ways in which the law can regulate both human and artificial behaviors, we should distinguish between the traditional technique of rules that hinge on the menace of legal sanctions and techno-regulation, that is, legal regulation by design. For example, the intent of the law to govern both human and robot behaviors can be divided into four different categories, that is, (a) the regulation of human producers and designers of robots through law, e.g., either through ISO standards or liability norms for users of robots; (b) the regulation of user behavior through the design of robots, that is, by designing robots in such a way that unlawful actions of humans are not allowed; (c) the regulation of the legal effects of robot behavior through the norms set up by lawmakers, e.g., the effects of robotic contracts and negotiations; and, (d) the regulation of robot behavior through design, that is, by embedding normative constraints into the design of the AA.[6] This differentiation can be complemented with further work on how the environment of the human-AA interaction can be regulated, and the legal challenges of "ambient law."[7] Accordingly, attention

[3] An overview in Pagallo (2013a, 2015a).

[4] See Koops (2006).

[5] See Reed (2012).

[6] See Leenes and Lucivero (2016).

[7] Check, among others, the work of Hildebrandt and Koops (2010), and Hildebrandt (2011).

should be drawn to the set of values, principles, and norms that constitute the context in which the consequences of such regulations have to be evaluated. The stronger the social cohesion is, the higher the risk in the automation process that can be socially accepted through the normative assessment of not fully predictable consequences of tasks and decisions entrusted to machines and AAs.[8]

By insisting on the different purposes and techniques of the law, however, we should prevent a twofold misunderstanding. The focus on the regulatory goals of the law does not mean either that the role of other regulatory systems should be underestimated, or that we can simply ignore the impact of technological innovation on the formalisms of the law. The relation between law and technology should on the contrary be grasped as the interaction between competing regulatory systems that not only may reinforce or contend against each other, but against further regulatory systems, such as the forces of the market and of social norms. Every regulatory system claims to govern social behavior by its own means, and can even render the claim of another regulatory system superfluous.

Reflect on the cases in which the legal intent to regulate the process of technological innovation has failed. A good example is given by the EU E-Money Directive 46 from 2000. Soon after its implementation, further forms of online payments, such as PayPal, forced the Brussels legislator to intervene, finally amending themselves with the new Directive 110 from 2009. Likewise, think of the legal umbrella for the adoption of such automatic techniques as digital right management (DRM), i.e., Article 8 of WIPO's 1996 *Copyright Treaty* and Article 14 of the twin *Performances and Phonograms Treaty*, which enable copyright holders to monitor and regulate the use of their protected artifacts. Twenty years after such international agreements, it seems fair to affirm these legal rules have fallen short in coping with people's behavior online and the dynamics of technological innovation, e.g., the introduction of *Cascading Style Sheets* (CSS)-technology to protect DVD artifacts, soon after followed by its DeCSS antidote. In this cat-and-mouse game, we can repeat what Steve Jobs said in his *Thoughts on Music*: "DRMs haven't worked, and may never work, to halt music piracy."[9]

On the other hand, the fields of AI and robotics abound with examples of how technological innovation may impact on pillars of the law. In addition to the use of AI systems and robots on the battlefield—and whether lethal force can be fully and legally automated—suffice it to mention the "contract problem." The current traditional interpretation of this legal issue conceives robots and other software agents as tools of social interaction. This means that rights and obligations established by the AA directly bind the human principal (P), since all the acts of AA are considered as acts of P; and moreover, P cannot evade liability by claiming either she did not intend to conclude such a contract or AA made a decisive mistake. In this latter case, e.g., in case of the erratic behavior of AA, what P can do is to claim damages against the designer and producer of AA. According to the mechanism of

[8]See Pagallo and Durante (2016).

[9]Jobs (2007), p. 3.

the burden of proof, P will have to demonstrate that AA was defective and that such defect existed while AA was under the manufacturer's control; and furthermore, the defect was the proximate cause of the injuries suffered by P.

Still, it is difficult to accept that rights and obligations established by AAs would be directly conferred upon humans, because the principal wanted the specific content, or agreement, of the contract made by AA. Rather, rights and obligations are conferred onto humans because they delegate to AA the authority to act on their behalf. Whereas the traditional approach that hinges on forms of strict liability ends up in a Hegelian night where all kinds of responsibility look grey, it seems necessary to amend today's rules of the law, so that operators and users of AAs should be held accountable in accordance with the different errors of the machine and the circumstances of the case. For example, humans should not be able to avoid the usual consequence of robots making a decisive mistake, i.e., the annulment of a contract, when the counterparty had to have been aware of a mistake that due to the erratic behavior of the robot, clearly concerned key elements of the agreement, such as the market price of the item or the substance of the subject-matter of that contract. In general terms, the aim should be to strike a balance between individuals claiming that they should not be ruined by the decisions or behavior of their AAs and the counterparties of such machines, demanding the ability to safely interact with them. This is the balance that has been aimed at by an increasing number of scholars over the past years.[10]

The current drawbacks of legal regulation should not be undervalued. However, the previous examples on how the goal of the law to govern the process of technological innovation miserably fails sometimes, do not suggest that we have to embrace the claims of techno-determinism, namely, the thesis that the race of technology is so determined and powerful that it cannot be deterred by legal means.[11] Rather, we have to take today's default rules of strict liability seriously, since this method of accident control may hinder further research in AI and robotics, and moreover trigger a vicious circle.

On the one hand, we already stressed above in the introduction, that robots and other AAs are not a simple "out of the box machine." On the other hand, we often lack enough data on the probability of events, their consequences and costs, to determine the levels of risk and, thus, the amount of insurance premiums and further mechanisms, on which new forms of accountability for the behavior of such machines may hinge. This lack of data is crucial, because the unpredictable and risky behavior of AAs can affect traditional tenets of the law, such as notions of reasonable foreseeability and due care, on which people's responsibility may depend. Yet, the more the strict liability rules of the law are effective, the less we can test our robots and correspondingly, the less we can comprehend how notions

[10]See, for example, Allen and Widdison (1996), Kerr (2001), Barfield (2005), Andrade et al. (2007), Sartor (2009), Pagallo (2013a).

[11]Among advocates of techno-determinism, see Moravec (1999), Kurzweil (2005), or Kelly (2010).

of reasonable foreseeability and due care may evolve in the next future. As a result, we need to further scrutinize this specific goal of the law, i.e., accident control through strict liability rules and the precautionary principle. The intent of Sect. 3 is to fully appreciate the terms of a possible legal deadlock. Then, Sect. 4 explores how we can tackle this vicious circle through the secondary rules of the law.

3 Primary Legal Rules for Accident Control

Theoretically speaking, there are three different kinds of legal agency that we have to examine in the field of AI and robotics. Since some of these machines do act, as stressed above in the introduction of this paper, such artificial agents can be conceived of (i) as proper persons with rights and duties of their own; (ii) as strict agents in the business law-field, e.g., in contract law and negotiations; and, (iii) as a source of responsibility for other agents in the system.

As to the hypothesis of AAs as proper legal persons, there has been an interesting debate on this topic over the past decades. However, at the risk of being lambasted for reactionary anthropocentrism, we can skip here this kind of debate.[12] Current legal systems have other kinds of priority, e.g., the employment of robo-soldiers and AI lethal systems on the battlefield, over whether granting personhood to AAs would provide for a more coherent picture of today's legal framework, whether we should prevent the ethical aberration of smart AAs being treated as mere slaves, or whether or not we can "rule out in advance the possibility that AIs (artificial intelligences) should be given the rights of constitutional personhood."[13]

As to the opinion that certain AAs should be conceived as strict agents in the business law-field, we already mentioned that most scholars and current legal systems present such AAs as simple tools of social interaction. This stance is however problematic—ending up in a Hegelian night where all kinds of responsibility look grey—so that an increasing number of experts have proposed a more equitable balance between the parties to a contract. We return to these proposals below in this section.

Finally, focus is on the third type of legal agency, i.e., robots and AI systems as a source of responsibility for other agents before the law. This level of abstraction corresponds to a popular point in jurisprudence, according to which AAs are neither legal persons nor proper agents, but rather a source of liability for the behavior of others. Some draw an analogy between strict liability policies for damages caused by animals and human liability for the behavior of their AAs, because the alleged novelty of all these latter cases resembles the responsibility of an owner or keeper of

[12]More details in Pagallo (2013a), pp. 155 et seq.

[13]Solum (1992), p. 1260.

an animal "that is either known or presumed to be dangerous to mankind."[14] Others propose the use of the traditional relations between principal and agent, master and servant, parent and child, warden and prisoner, down to keeper and animal, so as to understand how we can figure out the individual's negligent-based liability for the behavior of (some types of) AAs.[15] Whatever the analogy we endorse, e.g., no-fault responsibility of humans for harm provoked by their animals, children or employees, the economic rationale for this legal regime is that strict liability rules represent the best method of accident control by scaling back dangerous activities.[16]

Still, this accountability varies in accordance with the type of application with which we are dealing, so that different types of strict liability follow as a result. Consider for example an ISO 8373 industrial robot, or a da Vinci surgery system in the medical sector. Whilst strict liability rules apply to most producers and designers of robots for how such machines are built to fulfill their task specifications, such a responsibility can be imposed for injuries that either are caused by the defective manufacture or malfunction of the machine, or by defects in its design. Depending on the circumstances, the burden of proof varies as a result.[17] In cases of defective manufacture of the robot, or deficiencies of its design, the burden of proof falls on the plaintiff who has to prove that the product was defective; that such defect existed while the product was under the manufacturer's control; and finally, that the defect was the proximate cause of the injuries suffered by the plaintiff. In cases of strict malfunction liability, responsibility can be imposed although the plaintiff is not able to produce direct evidence on the defective condition of the product or the precise nature of the product's defect. Rather, the plaintiff is to demonstrate that defect through circumstantial evidence of the occurrence of a malfunction, or through evidence eliminating both abnormal use of the product and reasonably secondary causes for the accident. In addition, responsibility may hinge on civil (as opposed to criminal) negligence that concerns the duty to conform to a certain standard of conduct. Accordingly, the plaintiff has to prove that defendants breached that duty, thereby provoking an injury and an actual loss or damage to the plaintiff.

As to responsibilities of end-users, the distinction between the military and civilian sectors appears crucial.[18] In the first case, although military commanders and competent political authorities should be held strictly responsible for all the decisions of robots and AI systems, conditions and clauses of immunity are established by conventions on the laws of war and International Humanitarian Law (IHL). As Philip Alston stressed in the 2010 Report to the UN General Assembly on extrajudicial, summary or arbitrary executions, "a missile fired from a drone is

[14]Davis (2011), p. 171.

[15]See Chopra and White (2011), especially Chap. 4.

[16]This is of course the stance of, e.g., Posner (1988).

[17]For the sake of conciseness, the analysis takes into account the primary rules of the US legal system. A comparison with further legal systems and their rules on liability and burdens of proof is developed in Pagallo (2013a).

[18]See, for example, Pagallo (2011, 2012).

no different from any other commonly used weapon, including a gun fired by a soldier or a helicopter or gunship that fires missiles. The critical legal question is the same for each weapon: whether its specific use complies with IHL."[19] Remarkably, NGOs and experts of international law still discuss the set of parameters and conditions that should strictly regulate the use of robot soldiers and AI systems on the battlefield and moreover, whether a new international agreement is necessary.[20] In any event, immunity policies should be conceived of as a last resort option that, in most legal systems, does not extend to state contractors (e.g., 28 U.S.C. § 2671).

On the other hand, as to the end-users of robots and AI systems in the civilian sector, attention should be drawn to some of the AI domestic assistants and software agents, home security and surveillance applications, mentioned above in the introduction. Pace traditional patterns of responsibility for the behavior of other agents in the legal system, matters of liability change vis-à-vis such AAs. The more these artificial agents are adaptable, interactive and autonomous, the more users will find it difficult to prove that the manufacturer of the AA did not conform to a certain standard of conduct, or that the supplier did not guard against foreseeable harm. Here it is likely that, especially in the field of tort law, responsibility for the behavior of these AAs will increasingly depend on the ways in which end-users train, treat, or manage their artificial companions. Regardless of whether the case concerns negligence-based responsibility or strict liability of humans, the mechanism of attributing to the parties the burden of proof varies with the type of stance we endorse. This variation brings us back to the traditional view of legal robotics and the aforementioned analogy between robots and, say, animals, children, or employees. For example, we may compare domestic robots with children under the responsibility of their parent, as in American law. Therefore, defendants need to prove their machine did not present any dangerous propensity or trait that is not typical of similar applications, even though, for the foreseeable future, little room would be left for defendants to prevent liability. Alternatively, we may compare robots with children under the responsibility of parents as in Italian law. In this case, defendants avoid responsibility when evidence shows that they could not prevent the harmful behavior of the AA, or that a fortuitous event occurred.

However, it is the parallel between domestic robots and AI employees that prevails in most legal systems. This means that the vicarious liability of the user would not let humans evade responsibility, once the plaintiff brings evidence of a legally sufficient condition. This legal outcome is in agreement with the opinion of those scholars that consider either robots as dangerous animals, or their use as an ultra-hazardous activity.[21] Of course, legal systems could also endorse forms of limited liability, so as to prevent the risk that individuals think twice before

[19]In Pagallo (2013a), p. 59.

[20]Suffice it to mention Melzer (2008), Wagner (2014), Bergen and Rothenberg (2015), Crawford (2016), Ohlin (2016).

[21]Davis (2011), p. 171.

employing robots that, in the phrasing of the UN Report of Robotics, will provide "services useful to the well-being of humans."[22] Some of the proposals mentioned above in the previous section—in order to strike a fair balance between the parties to a contract—could thus be expanded to the field of tort law and extra-contractual obligations. Some argue that we should register such machines just like corporations[23]; others suggest that we should bestow robots with capital,[24] or that making the financial position of such machines transparent is a priority.[25] Whilst further policies are feasible and even indispensable, e.g., insurance models and what I elsewhere called the "digital peculium" of robots,[26] it is nonetheless clear that the aim of the law should be to strike a balance between the individual's claim to not be ruined by the decisions of their AAs and the claim of an AA's counterparty to be protected when interacting with them.

Yet, lest we change current default rules of the law on the vicarious responsibility of users for the decisions of their smart artificial companions, there is a major problem. Since users cannot evade liability vis-à-vis evidence of a legally sufficient condition, e.g., claiming that any injuries, damages or harm caused by their AAs was reasonably unforeseeable, individuals will be discouraged from buying and using such AAs at all. The capability of such machines to gain knowledge and skills from interaction with human caretakers, suggests that the fault would rarely fall on designers, manufacturers or suppliers of such AAs. Rather, according to the rationale for strict liability rules, it could be argued that owners or users of AAs are in the best position to understand what is going on with the machine. Therefore, it is up to end-users to prevent the dangerous behavior of the AA, regardless of whether the conduct of the robot, or of other AI system, was typical of similar AAs, reasonably predictable and so forth. In the long run, i.e., after two or three generations of AI domestic assistants and software agents, interacting with their human masters, we can suspect that the duty of humans to take care of such machines will not be deemed similar to the current responsibility to control the dangerous propensities of animals and children. Yet, the question can be raised whether users and owners of, e.g., home security and smart surveillance applications need to wait for the long run in order to be finally reckoned as the reasonable person of today's tort law.

The breath-taking progress in the fields of AI and robotics vis-à-vis the current primary rules of the law brings back to the vicious circle illustrated in the previous sections of this work. On the one hand, experts and international organizations alike

---

[22]See UN (2005).

[23]This is the opinion of Karnow (1996), Lerouge (2000), or Weitzenboeck (2001).

[24]The thesis is developed in Bellia (2001).

[25]This is the claim of Sartor (2009).

[26]See Pagallo (2013a), pp. 103 et seq. Drawing on ancient Roman law, the overall idea of the peculium is, on the one hand, that individuals that employ AAs to do business, transactions or contracts, could claim a liability limited to the value of their AAs portfolio (plus, eventually, forms of compulsory insurance). On the other hand, the AAs' peculium would guarantee their human counterparties, or other AAs, that obligations would really be met.

have stressed time and again the whole set of opportunities, affordances, and benefits brought on by AI systems and robotics technology. In the "Robotics 2020 Strategic Research Agenda" of the EU Commission, the latter insists on the benefits of such apps that "range from helping the elderly stay safely mobile in their own homes to the automation of everyday household chores and the provision of remote monitoring and security for home."[27] On the other hand, the risk is that legislators can make individuals think twice before using or producing robots and further AAs, through methods of accident control that cut back on the scale of the activity via strict liability rules. Moreover, the goal of the law can even be to prevent such activities at all, through the precautionary principle. By shifting the burden of proof from those suspecting a risk in the construction and use of AAs, to those who discount that risk, the principle basically states that we should prevent action when there is not (scientifical) certainty that no dangerous effect would ensue.

Consider again the da Vinci surgery systems: in this case, producers of such applications had to pro-actively demonstrate that the commercialization and use of robots for medical purposes is satisfactorily safe. On the basis of scientific evidence, Intuitive Surgical could thus obtain the authorization of the U.S. Food and Drug Administration, e.g., approval Z-0658-2008 for "the Class 2 Recall da Vinci Surgical System 8 mm Long Instrument cannula." Likewise, in the EU legal system, the burden of proof falls on producers and manufacturers of unmanned aircrafts, or drones, that should preventively demonstrate "their capability and means of discharging the responsibilities associated with their privileges." In the wording of Article 8 (2) of the EU Regulation 216/2008 on common rules in the field of civil aviation and establishing a European Aviation Safety Agency (EASA), "these capabilities and means shall be recognized through the issuance of a certificate. The privileges granted to the operator and the scope of the operations shall be specified in the certificate."

Yet, applications of this principle can be harsher and with overall intent. The recent wave of extremely detailed regulations and prohibitions on the use of drones by the Italian Civil Aviation Authority, i.e., "ENAC," illustrates this deadlock.[28] The paradox stressed in the field of web security decades ago, could be extended with a pinch of salt to the Italian regulation on the use of drones as well: the only legal drone would be "one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards—and even then I have my doubts."[29] As a result, we often lack enough data on the probability of events, their consequences and costs, to determine the levels of risk and thus, the amount of insurance premiums and further mechanisms on which new forms of accountability for the behavior of a new generation of drones and, generally speaking, of AAs could hinge. As a US Navy-sponsored research admitted some years ago, "we may

[27]EU Commission (2013), p. 34.

[28]See Pagallo (2016).

[29]See the introduction of Garfinkel and Spafford (1997).

paradoxically need to use the first deaths to determine the level of risk."[30] What is intolerable in the military sector is even more unacceptable in the civilian field. How, then, to prevent legislations that may hinder the research in AI and robotics? How to deal with their peculiar unpredictability and risky behavior? How should we legally regulate the future?

4 Secondary Legal Rules for Accident Control

So far, the analysis of this work has concerned the primary rules of the law that aim to govern individual and social behavior, both human and artificial. This level of analysis has regarded today's default rules of strict liability in the fields of contracts and tort law, immunity in IHL and the laws of war, and how we could tackle some of their drawbacks. For instance, in the law of wars, an effective treaty monitoring and verification mechanisms should allow through a detailed set of parameters, clauses and rules of engagement, for a determination of the locus of political and military decisions that the increasing complexity of network centric operations and the miniaturization of lethal machines can make very difficult to detect. In the field of contracts, it seems reasonable to expect that the humans involved in transactions with software agents and robo-traders should be bound by the interpretation of the behavior of such AAs that usually applies to the circumstances of the case according to existing conventions of business and civil law. In tort law, we could amend current clauses of vicarious responsibility with policies of compulsory insurance and forms of limited liability, such as the digital *peculium*, in order to strike a fair balance in distributing responsibility and risk.

However, these different ways to adjust current legal frameworks, especially in the fields of business and tort law, face a problem, namely a variant of the vicious circle stressed throughout the previous sections of this work. Whereas, on the one hand, new models of limited accountability and insurance policies need data on the probability of events, their consequences and costs, on the other hand the more current default rules of strict liability are effective, the less we can test our AAs and obtain the data for these new models of accountability, etc. This scenario appears even worse with some applications of the precautionary principle that may lead to irrational, protectionist, risk-averse or simply paradoxical outcomes. Consider the classic epistemological argument of Karl Popper's falsificationism, i.e., the assumption that, from a logical viewpoint, a scientific theory cannot conclusively be verifiable, although it shall conclusively be falsifiable.[31] Hence, in the case of the precautionary principle, we may invoke a sort of "reversed Popperian paradox," since the need of proving the absence of risk before taking action, rather than proving the existence of such risk, implies that inactivity would continue until a

[30]The paradox is stressed by Lin et al. (2007).

[31]The reference is, of course, Popper (1935/2002).

no-evidence hypothesis is falsified. How then, should we approach this number of vicious circles, paradoxes, and drawbacks?

A smart way to address these issues suggests another level of analysis: attention should be drawn to the secondary rules of the law that create, modify, or suppress the primary rules of the system.[32] Noteworthy, this is how the Japanese government has worked out a way to tackle the normative challenges of robotics through the creation of special zones for empirical testing and development, namely, a form of living lab, or *Tokku*. After the Cabinet Office approved the world's first special zone in November 2003, covering the prefecture of Fukuoka and the city of Kitakyushu, further special zones have been established in Osaka and Gifu, Kanagawa and Tsukuba. The overall aim of these special zones is to set up a sort of interface for robots and society, in which scientists and common people can test whether robots fulfill their task specifications in ways that are acceptable and comfortable to humans vis-à-vis the uncertainty of machine safety and legal liabilities that concern, e.g., the protection for the processing of personal data.[33] Significantly, this approach to the risks and threats of human-robot interaction is at odds with the formalistic interpretation of the law often adopted in Japan. Moreover, it is remarkable that such special zones are highly deregulated from a legal point of view. "Without deregulation, the current overruled Japanese legal system will be a major obstacle to the realization of its Robot Tokku (RT) business competitiveness as well as the new safety for human-robot co-existence."[34] Furthermore, the intent is "to cover many potential legal disputes derived from the next-generation robots when they are deployed in the real world."[35]

So far, the legal issues addressed in the RT special zones regard road traffic laws (Fukuoka 2003), radio law (Kansai 2005), privacy protection (Kyoto 2008), safety governance and tax regulation (Tsukuba 2011), up to road traffic law in highways (Sagami 2013). These experiments could obviously be extended, so as to strengthen our understanding of how the future of the human-robot interaction and further AAs could turn out with some of the issues examined in the previous sections, such as matters of foreseeability and due care, or the unpredictability of robotic behavior that may trigger novel forms of negligence in tort law. By testing this interaction outside laboratories, i.e., in open or unstructured areas, this approach does not only show a pragmatic way to tackle the legal challenges of AI and robotics. This sort of interface between stronger AI robots and human societies, between present and future, represents the legal basis on which to collect empirical data and sufficient knowledge to make rational decisions for a number of critical issues. First, we can improve our understanding of how these AAs may react in various contexts and

[32]For the distinction between primary and secondary legal rules, see Hart (1961). In this context, we can leave aside such secondary rules, as the rules of recognition and of adjudication, so as to focus on the rules of change.

[33]Further details in Pagallo (2013b).

[34]Weng et al. (2015), p. 850.

[35]Weng et al. (2015), p. 850.

satisfy human needs. Second, we can better appreciate risks and threats brought on by possible losses of control of AI systems, so as to keep them in check. Third, we can further develop theoretical frameworks that allow us to better appreciate the space of potential systems that avoid undesirable behaviors. Four, we can rationally address the legal aspects of this experimentation, covering many potential issues raised by the next-generation AAs and managing such requirements, which often represent a formidable obstacle for this kind of research, as public authorizations for security reasons, formal consent for the processing and use of personal data, mechanisms of distributing risks through insurance models and authentication systems. As stressed by the Committee on Legal Affairs of the European Parliament in the recommendations to the EU Commission on civil law rules on robotics from May 31 2016, "testing robots in real-life scenarios is essential for the identification and assessment of the risks (that AI & robots) might entail, as well as of their technological development beyond a pure experimental laboratory phase."[36]

In addition to these legally deregulated special zones, other aims we may attain through the secondary rules of the law can be mentioned. Some of these functions converge with the legal and experimental purposes of the special zones. Consider Article 35 of the EU general data protection regulation (GDPR) n. 679 from 2016, on a new generation of privacy impact assessments and the powers of the supervisory authorities pursuant to Article 36 of GDPR. Here, the idea is to pre-emptively assess the impact of new technologies on the processing of personal data, so as to minimize or prevent any kind of "risk to the rights and freedoms of natural persons." Some others propose a sort of Federal Robotics Commission in the US as the appropriate institution for coordinating governance of robotics and moreover, accelerating the accumulation of federal expertise in the field, since governments often are ill-equipped to deal with ongoing AI developments.[37] Such a Federal AI and Robotics Commission, in other words, should "coordinate an on-going government-wide initiative to investigate possible AI futures, drawing on the best methods in technological forecasting and scenario planning, and to also investigate both how agencies can leverage such technologies for the public good, and how critical mission areas could be affected by AI should adjust based on such futures."[38]

Further examples of this approach to the normative challenges of AI and robotics could be given. But, to cut to the chase, let us sum up the role of the secondary rules for accident control, according to three main motives. First, the secondary rules of the law help us understand what kind of primary rules we may wish, especially when we are confronted with cases of disagreement, such as matters of reasonable foreseeability and due care in the law of torts. Second, the secondary rules of the law allow us to find out several ways in which we can tackle the vicious circle triggered by current rules of strict liability and the subsequent lack of data. By

[36]N. 14 of the doc. 2015/2103(INL).

[37]See, e.g., Calo (2014).

[38]Brundage and Bryson (2016), p. 6.

gathering and evaluating crucial data on the probability of events, their consequences and costs, we can complement, or even contrast, current rules for accident control. New forms of accountability for the behavior of robots and other AAs can be formulated on the basis of a more precise understanding of the levels of risk on which, e.g., the amount of insurance premiums have to be determined. Third, the secondary rules of the law also allow us to tackle the threshold for applying the precautionary principle, namely, the existence and degree of scientific uncertainty as to the harm that the use of sensitive technology might invoke.

However, the different ways in which the secondary rules of the law may interact with its primary rules, seem to trigger a new set of problems. Can the secondary rules of the law help us solve all of the problems of ignorance, lack of data, or general disagreement among scholars, that piled up in the previous sections of this work? Moreover, could the functioning of the secondary rules provide a new basis for the idea that jurists could apply the principles of the law in such a way that presents every case at hand in the best possible light?

The time is ripe for addressing this final set of issues in the conclusion of the analysis.

5 Conclusion

This chapter has dwelt on the normative challenges of AI and robotics, and the aim of the law to govern the process of technological innovation (Sect. 2). More particularly, the focus was on today's clauses and conditions of responsibility/liability in the legal field (Sect. 3). This stricter perspective on the primary rules of the system that govern individual conduct, emphasized three cases which are under stress:

1. Clauses of immunity in the laws of war and IHL, and whether we should amend them through a new international agreement;
2. AAs as simple means of human interaction in contract law, and whether we should hold operators and users of AAs accountable in accordance with the different errors of the machine and the circumstances of the case;
3. Vicarious responsibility of users for the decisions of AAs in the field of torts, and whether another kind of balance should be struck between the different human interests involved in extra-contractual obligations.

The attention was thus drawn to that which jurists usually sum up as their legal "hard cases,"[39] that is, cases of general disagreement that may regard the meaning of the terms framing the question, the ways such terms are related to each other in legal reasoning, or the role of the principles that are at stake in the case. These cases are particularly relevant for they produce a form of meta-disagreement on how we

[39]See, e.g., Hart (1961), and Dworkin (1985).

should grasp the hard cases of the law.[40] On the one hand, Dworkin and his followers have suggested the uniquely right answer-approach. According to this stance, a morally coherent narrative should grasp the law in such a way that, given the nature of the legal question and the story and background of the issue, scholars can attain the answer that best justifies or achieves the integrity of the law.[41] By identifying the principles of the system that fit with the established law, jurists could apply such principles in a way that presents the case in the best possible light. On the other hand, some oppose this argument because a class of legal cases would confront us with something new that requires a thoughtful agreement between different opinions. In the words of the most important advocate of this stance, "there is no possibility of treating the question raised by the various cases as if there were one uniquely correct answer to be found, as distinct from an answer which is a reasonable compromise between many conflicting interests."[42]

Arguably, today's debate on whether lethal force should ever be permitted to be fully automated, i.e., the first of our hard cases, seems to support Hart's views. Some propose the ban on every "autonomous weapon,"[43] while others argue against such a ban because AI systems and robotic weapons might lead to less civilian deaths.[44] In light of this debate, however, we do not have to buy any of Hart's theoretical assumptions on, say, the rule of recognition and the minimum content of natural law, to admit that a reasonable compromise seems necessary. Since 2015, after all, the UN has been working on the details that should govern the use of robot soldiers and AI systems in battle. Whereas previous international agreements have regulated technological advancements over the past decades in such fields as chemical, biological and nuclear weapons, or the field of computer crimes since the early 2000s, an effective treaty monitoring and verification mechanisms appear necessary to define the locus of political and military decisions that advancements in AI and robotics technology can make difficult to determine.[45]

As to the further hard cases of the analysis on the laws of contracts and torts, things are different. Current default rules of strict liability—as opposed to clauses of immunity in the laws of war—may hinder research in AI and robotics applications that provide services useful to the well-being of humans. As stressed throughout this chapter, today's legal framework ends up with a vicious circle, because the more current default rules of strict liability are effective, the less we can test our

[40]For a useful introduction, see Shapiro (2007).

[41]In addition to Dworkin (1985), see Dworkin (1986).

[42]Hart (1961), p. 128.

[43]See, e.g., Human Rights Watch (2012).

[44]Among others, this is the thesis of Lin et al. (2007), or, Toscano (2015).

[45]It must be admitted that a new international agreement on some critical aspects of today's laws of war may not only take a long time, but this stalemate will likely continue as long as sovereign states think they can exploit the loopholes of the current legal framework due to their technological superiority or strategic advantage. However, the lack of an international agreement does not entail a new Hobbesian state-of-nature of the information era, in which all is permitted among sovereign states. See Pagallo (2015b).

AAs and obtain the data for new models of accountability and insurance policies with which we may amend, or change, today's primary rules. In order to find a feasible way out to this legal deadlock, Sect. 4 has proposed to pay attention to the secondary rules of the system, e.g., setting up legally deregulated special zones for AI and robotics empirical testing and development that should allow us to understand what kind of primary legal rules we may need. Although this approach represents a smart way to tackle the normative challenges of AI and robotics, the interaction between primary and secondary rules of the law can however be grasped in a twofold way.

The first stance is compatible with the tenets of the Dworkinian right answer-thesis. Whereas we may admit cases of ignorance and lack of data that suggest the adoption of specific secondary rules to address the difficulty of these cases, the aim of the secondary rules can be to set up the conditions for improving our comprehension of the primary rules that can best justify the integrity of the law. Yet, this kind of experimentation through the secondary rules of the law does not guarantee any uniquely right-answer as to the content of the primary rules of the system. After the phase of legal experimentation, general disagreement may persist and revolve around the goals of legislation, for example whether the law should endorse non-discrimination between technologies with equivalent effects, or favor specific solutions over other technological alternatives. Moreover, we may consent to a given goal of legislation and still, differ in how we could attain that end. Going back to the example of robo-traders, as stressed above in Sect. 3, we can agree on mitigating today's rules of strict liability in the field of contracts and nevertheless, disagree on whether the priority should be making the financial position of such AI machines transparent, bestowing robots with capital, registering such AAs just like corporations, and more. From a Hartian point of view, however, this further level of disagreement is not disturbing. As occurs with the first of our hard legal cases on robo-soldiers and AI systems on the battlefield, this kind of contention would confirm that at times reasonable compromises have to be found in the legal domain.

On this basis, let us summarize the analysis of this chapter with three different ways in which we can inflect its title: LegalAIze, first, refers to the vicious circle of current strict liability rules and the paradoxes of the precautionary principle that should be tackled through the secondary rules of the law, e.g., setting up special zones for AI and robotics empirical testing and development. If we are fated to face some of the scenarios sketched above in the paper, e.g., negligence of humans as caretakers of their AAs, we should address these scenarios, first, in a living lab.

Second, LegalAIze concerns the set of alternatives proposed to the current legal framework, in accordance with a Dworkinian methodology. In light of the normative challenges of AI and robotics, it seems fair to assume that lawyers should start thinking about the law in a morally coherent way, in order to propose the solution that best fits the principles and norms of the system through models of accountability, transparency, authentication systems, and the like. At times, luckily enough, we deal with cases where legal issues appear "plain," that is, "where the

general terms seem to need no interpretation and where the recognition of instances seems unproblematic or 'automatic'… where there is general agreement in judgments as to the applicability of the classifying terms."[46] If this is not the case, for disagreement arises among scholars, the next step is to ascertain whether or not a uniquely right-answer is at hand. Should we be good enough to flesh out the right answer through our own analysis, e.g., the digital *peculium* for some kinds of robots and AI systems,[47] let us adopt it.

Third, LegalAIze has to do with the reasonable compromises that, now and then, are necessary in the legal field. The intent should be to strike a balance between the counterparties of AAs demanding the ability to safely interact or transact with such machines and individuals claiming that they should not be ruined by the decisions or behavior of their own robots and AI systems. The secondary rules of the law offer a practical way to increase and strengthen our comprehension of what should be deemed as reasonable. Since AAs are here to stay, the aim of the law should be to wisely govern our mutual relationships.

References

Allen C, Varner G, Zinser J (2000) Prolegomena to any future artificial moral agent. J Exp Theor Artif Intell 12:251–261

Allen T, Widdison R (1996) Can computers make contracts? Harv J Law Technol 9(1):26–52

Andrade F et al (2007) Contracting agents: legal personality and representation. Artif Intell Law 15:357–373

Barfield W (2005) Issues of law for software agents within virtual environments. Presence 14 (6):741–748

Bellia AJ (2001) Contracting with electronic agents. Emory Law J 50:1047–1092

Bergen PL, Rothenberg D (2015) Drone wars: transforming conflict, law, and policy. Cambridge University Press, Cambridge

Brundage M, Bryson J (2016) Smart policies for artificial intelligence. Cornell University Library. https://arxiv.org/abs/1608.08196v1. Accessed 24 Sept 2016

Calo R (2014) The case for a federal robotics commission. Brookings Institution, Washington

Chopra S, White LF (2011) A legal theory for autonomous artificial agents. The University of Michigan Press, Ann Arbor

Crawford E (2016) The principle of distinction and remote warfare. Sydney Law School Research Paper No. 16/43

Davis J (2011) The (common) laws of man over (civilian) vehicles unmanned. J Law Inf Sci 21 (2):166–179

Dworkin R (1985) A matter of principle. Oxford University Press, Oxford

Dworkin R (1986) Law's empire. Harvard University Press, Cambridge

EU Commission (2013) Robotics 2020 strategic research agenda for robotics in Europe, draft 0v42, 11 Oct

Floridi L, Sanders J (2004) On the morality of artificial agents. Mind Mach 14(3):349–379

[46]Hart (1961), p. 121.

[47]See above note 26.

Franklin S, Graesser A (1997) Is it an agent, or just a program? A taxonomy for autonomous agents. In: Müller J, Wooldridge M, Jennings N (eds) Intelligent agents III, Proceedings of the third international workshop on agent theories, architectures, and languages, Springer, Berlin
Garfinkel S, Spafford G (1997) Web security and commerce. O'Reilly, Sebastopol
Hart HLA (1961) The concept of law. Clarendon, Oxford
Hildebrandt M (2011) Legal protection by design: objections and refutations. Legisprudence 5 (2):223–248
Hildebrandt M, Koops BJ (2010) The challenges of ambient law and legal protection in the profiling era. Mod Law Rev 73(3):428–460
Human Rights Watch (2012) Losing humanity: the case against killer robots. https://www.hrw.org/report/2012/11/19/losing-humanity/case-against-killer-robots. Accessed 24 Sept 2016
Jobs S (2007) Thoughts on music. http://www.apple.com/hotnews/thoughtsonmusic/. Accessed 24 Sept 2016
Karnow CEA (1996) Liability for distributed artificial intelligence. Berkeley Technol Law J 11:147–183
Kelly K (2010) What technology wants. Viking, New York
Kerr I (2001) Ensuring the success of contract formation in agent-mediated electronic commerce. Electron Commer Res J 1:183–202
Koops BK (2006) Should ICT regulation be technology-neutral? In: Koops BJ et al (eds) Starting points for ICT regulation: deconstructing prevalent policy one-liners. TMC Asser, The Hague
Kurzweil R (2005) The singularity is near. Viking, New York
Leenes R, Lucivero F (2016) Laws on robots, laws by robots, laws in robots: regulating robot behaviour by design, law. Innov Technol 6(2):193–220
Lerouge JF (2000) The use of electronic agents questioned under contractual law: suggested solutions on a European and American level. John Marshall J Comput Inf Law 18:403
Lin P, Bekey G, Keith A (2007) Autonomous military robotics: risk, ethics, and design. Report for US Department of Navy. Office of Naval Research. Ethics + Emerging Sciences Group at California Polytechnic State University, San Luis Obispo
Melzer N (2008) Targeted killing in international law. Oxford University Press, Oxford
Moravec H (1999) Robot: mere machine to transcendent mind. Oxford University Press, London
Ohlin JD (2016) Remoteness and reciprocal risk. Cornell Legal Studies Research Paper No. 16–24
Pagallo U (2011) Robots of just war: a legal perspective. Philos Technol 24(3):307–323
Pagallo U (2012) Guns, ships, and chauffeurs: the civilian use of UV technology and its impact on legal systems. J Law Inf Sci 21(2):224–233
Pagallo U (2013a) The laws of robots: crimes, contracts, and torts. Springer, Dordrecht
Pagallo U (2013b) Robots in the cloud with privacy: a new threat to data protection? Comput Law Secur Rev 29(5):501–508
Pagallo U (2015a) Good onlife governance: on law, spontaneous orders, and design. In: Floridi L (ed) The onlife manifesto: being human in a hyperconnected era. Springer, Dordrecht
Pagallo U (2015b) Cyber force and the role of Sovereign States in informational warfare. Philos Technol 28(3):407–425
Pagallo U (2016) Even angels need the rules: on AI, roboethics, and the law. In: Kaminka GA et al (eds) ECAI proceedings. IOS Press, Amsterdam
Pagallo U, Durante M (2016) The pros and cons of legal automation and its governance. Eur J Risk Regulation 7(2):323–334
Popper KR (1935/2002) The logic of scientific discovery, 2nd edn. Routledge, London
Posner R (1988) The jurisprudence of skepticism. Mich Law Rev 86(5):827–891
Reed Ch (2012) Making laws for cyberspace. Oxford University Press, Oxford
Sartor G (2009) Cognitive automata and the law: electronic contracting and the intentionality of software agents. Artif Intell Law 17(4):253–290
Shapiro SJ (2007) The 'Hart-Dworkin' debate: a short guide for the perplexed. Public Law and Legal Theory Working Paper Series 77, Michigan Law School

Solum LB (1992) Legal personhood for artificial intelligence. N C Law Rev 70:1231–1287
Toscano C (2015) "Friend of humans": an argument for developing autonomous weapon systems. J Natl Secur Policy 8:189–236
UN World Robotics (2005) Statistics, market analysis, forecasts, case studies and profitability of robot investment, edited by the UN Economic Commission for Europe and co-authored by the International Federation of Robotics. UN Publication, Geneva
Wagner M (2014) The dehumanization of international humanitarian law: legal, ethical, and political implications of autonomous weapons systems. Vanderbilt J Transnatl Law 47:1371–1424
Weitzenboeck EM (2001) Electronic agents and the formation of contracts. Int J Law Inf Technol 9(3):204–234
Weng YH et al (2015) Intersection of "Tokku" special zone, robots, and the law: a case study on legal impacts to humanoid robots. Int J Social Robot 7(5):841–857
Wooldridge MJ, Jennings NR (1995) Agent theories, architectures, and languages: a survey. In: Wooldridge M, Jennings NR (eds) Intelligent agents. Springer, Berlin

In the Shadow of Banking: Oversight of Fintechs and Their Service Companies

Daniel Bunge

Abstract In the United States, the regulatory authority of government agencies over financial institutions' third-party service providers varies depending on the type of financial institution. The Federal Depository Insurance Corporation (FDIC), the Board of Governors of the Federal Reserve System (FRB), and the Office of the Comptroller of the Currency (OCC) may extend their authority over service providers to their supervised institutions. Meanwhile, the National Credit Union Administration (NCUA) lacks this authority for credit unions. The federal and state agencies that oversee Money Service Businesses (MSBs) also lack this authority. The regulatory authority over MSBs service providers is particularly interesting because of the rise of virtual currency businesses providing an alternative payment rail outside of traditional institutions, allowing small fintech startups to enter into the payment space. This chapter examines federal and state authority over third-party service providers and justifications thereof. It goes on to examine some of the more unique aspects of fintech entrants to the payment space and how their service providers should be treated along with other MSBs. Ultimately, this chapter recommends that private contract law between MSBs and their service providers be used to mitigate the risks in their relationship. Limited resources and duplicative regulatory costs between federal and state agencies as well as the relatively small size of the industry makes it inefficient to directly supervise third-party service providers. However, this chapter does not reject the possibility of future extensions of government authority as the industry and its potential impact over the financial system grows.

Keywords Bitcoin · Financial technology · Technology service providers · Third-party service providers · Virtual currencies

D. Bunge (✉)
Attorney, New York, NY, USA
e-mail: daniel.r.bunge@gmail.com

M. Corrales et al. (eds.), *New Technology, Big Data and the Law*,
Perspectives in Law, Business and Innovation, DOI 10.1007/978-981-10-5038-1_12

Contents

1 Introduction

The rise of financial technology companies, or fintechs, has sparked the interest of bankers and the public alike. While technological innovation is nothing new to the financial industry, the latest epoch heralds a shift in focus to non-traditional financial companies. IT juggernauts like Apple, Samsung, and Google are developing their own mobile payment systems overlaid on financial institutions' traditional payment rails. Meanwhile, innovative technology startups such as Venmo and Square are targeting the same payment space hoping to improve customer experience and grab their own slice of the market. Finally, and most controversially, cryptocurrencies such as Bitcoin have shifted from a dark web currency used by criminals to a more legitimate phase,[1] attracting venture capital in the payment industry. These companies rely on payment rails that are not under the control of the financial industry. Indeed, most cryptocurrency networks are not controlled by any centralized institution.

While the fintechs involved in money transmission seek to take advantage of technological efficiencies to compete with the established institutions, a third-party service industry has grown around them. Platform providers such as BitGo provide an enterprise solution for blockchain businesses including anti-fraud features. Compliance services such as those offered by Chainalysis and Elliptic offer transaction monitoring and reporting to allow more transparent compliance with Anti-Money Laundering (AML) laws. Consulting services such as Ledger Labs review the security of blockchain-based businesses.

This chapter focuses on these third-party service providers, specifically the authority of federal and state regulatory agencies to supervise third-party service

[1]See, e.g., Tasca et al. (2016) (examining the characteristics of Bitcoin payments and their history, showing that the majority of payment has shifted from the "sin" industry of gambling and black markets to more legitimate businesses).

providers. This chapter compares the treatment of third-party service providers to Money Service Businesses (MSBs) to those that service other financial institutions such as national banks and credit unions. MSB and credit union service providers prove beyond the reach of most existing federal financial law.

Virtual currency MSBs are a subset of all Virtual Currency Businesses (VCBs). The term MSB service provider means a business that provide services to MSBs, but is not itself an MSB under federal law. MSB service providers are a subgroup of third-party service providers. The third-party service providers used by national banks, state banks, credit unions, and other such financial institutions include businesses that provide services such as payment processing, which would fall within the definition of MSB, but for an exemption. As payment processing services provided to an MSB would themselves fall under the definition of MSB, these services are excluded from the definition of MSB service provider.

This chapter is organized into the five following sections. Section 2 offers an overview of third-party service providers, their risks, and supervision. Section 3 provides a brief explanation of the distributed ledger technology used by virtual currency MSBs. Section 4 reviews federal and state laws with regard to extending supervisory authority over third-party service providers. Section 5 discusses how MSB service providers, especially those servicing virtual currency MSBs, create a challenge for regulators and the financial institutions that manage their risk. It then examines whether existing methods are sufficient to address this risk. Section 6 provides concluding remarks.

2 Third-Party Service Providers' Risks

Third-party service providers are employed by financial institutions for any number of purposes from accounting and legal services to payment processing and cybersecurity. As such, third-party service providers can permit these financial institutions to save on operating costs and enable smaller entities to conduct business where they would otherwise be unable to afford to develop the technology and expertise internally. However, by outsourcing activities to third-party service providers, financial institutions also expose themselves to additional risk. These risks can be organized into five categories.[2]

i. *Operational Risk*: the inherit risk of the product or service that may be compounded by the inability of the financial institution to exercise direct control over the third-party service provider;
ii. *Compliance Risk*: the risk of noncompliance with applicable laws and regulations as well as the financial institution's internal policies and procedures; By outsourcing to a third-party, a financial institution loses the ability to directly control these measures;

[2]U.S. Comptroller of the Currency (2013).

iii. *Reputation Risk*: the risk that poor performance on the part of the third-party service provider damages the financial institution's public image;
iv. *Strategic Risk*: the risk that the use of or failure to use a third-party service provider harms the financial institution's strategic business goals;
v. *Credit Risk*: the risk of default on a debt connected to third-party service provider activities performed on behalf of the financial institution such as origination, solicitation of customers, and underwriting research.

There are three groups that are interested in mitigating these risks. The first is the financial institutions themselves, the second is depository institutions providing accounts to these financial institutions, and the third is government regulatory agencies.

When entering into a relationship with a third-party service provider, a financial institution must take the above risks into account and evaluate how they can be managed by the financial institution and the third-party service provider. As such, conducting proper due diligence, establishing rights and duties through contract negotiation, and ongoing monitoring of the third-party service provider are all important in ensuring a successful relationship.

The risks of third-party service providers are not only considered by the financial institutions they work with. MSBs rely on depository institutions for many financial services such as bank accounts. The depository institutions providing these accounts are legally obligated to ensure there are proper policies in place against money laundering and other suspicious activity.[3] They would need to evaluate how the use of service providers affects an MSB's risk profile. Without transparency, depository institutions may choose to not provide accounts to MSBs.[4]

A final group interested in third-party service providers is government regulatory agencies. By regulating and examining third-party service providers directly, these agencies may be able to better ensure the safety, soundness, and legal compliance of MSBs.[5]

With the risks inherent in third-party service providers, it is important that MSBs be able to properly evaluate and mitigate these risks. The consequences of not vetting a service provider can be severe, ranging from losing access to banking services to government fines for non-compliance. The question is whether private contractual law is sufficient to mitigate these risks or whether it needs to be bolstered by direct government supervision. The next section discusses the technology behind virtual currencies and the risks that they may introduce into the financial system.

[3]31 CFR 1010.620. For a discussion of money laundering risk management for third-party payment processors. See Federal Financial Institutions Examination Council (2014), pp. 235–39.

[4]A recognized problem in the financial world is "de-risking." De-risking is the categorical refusal by depository institutions to provide accounts to entire classes of businesses without review of their individual risks and merits. See El-Hindi (2016). Virtual currency buisenesses have had an especially hard time, although being properly prepared to comply with relevant regulations and engage with bankers can mitigate this risk. See Vallabhaneni et al. (2016).

[5]See Sect. 4.

3 Blockchain Technology

Virtual currency such as Bitcoin rely on blockchain technology[6] that allows for verification of transactions without the need for trusted parties. As the variants of blockchains are numerous, including applications in the securities markets,[7] commodities markets,[8] and even timestamping contracts,[9] this chapter focuses only on those in the payment space. The first blockchain, Bitcoin,[10] is used by way of example, and then possible variations are discussed.[11] There are several important pieces of the Bitcoin protocol: cryptocurrency, nodes and consensus.

The cryptocurrency that is traded back and forth between different Internet users is denoted as "bitcoin" in all lower case. A cryptocurrency is a cryptographically protected virtual currency[12] and it shares many similarities with currency as we traditionally think of it.[13] That is, people can use it to pay for goods and services as a medium of exchange. People can, in turn, price their goods and services in bitcoin, using it as a unit of account. Finally, bitcoin may be saved instead of spent as a store of value. However, virtual currencies are not legal tender and have no government backing.[14]

It is important to understand that cryptocurrencies are not a fundamental part of blockchain technology. All that is sent is a digital token that can represent almost anything. For example, the digital token can represent a claim on fiat currency.[15]

---

[6]Often the term distributed ledger technology (DLT) is conflated with blockchain technology. DLT represents an electronic ledger that is shared between multiple devices. Blockchain technology uses DLT to implement the trustless transfer of electronic data as explained in this section.

[7]Australia Securities Exchange (ASX) is experimenting with using a private blockchain to replace its securities clearing and settlement system. See Wadhwa (2016). For a discussion of the advantages and disadvantages of using the blockchain to replace the existing security settlement system in the United States. See Depository Trust & Clearing Corporation (2016) and Society for Worldwide Interbank Financial Telecommunications (2016).

[8]Kynetix has launched a consortium along with 15 participants in the industry to look into applying blockchain technology to commodities. See Kendall (2015).

[9]Maltese (2015).

[10]As is industry standard, the capitalized "Bitcoin" is used to describe the protocol, while lowercase "bitcoin" is used to describe the cryptocurrency.

[11]The focus of this analysis is on blockchain used as a payment system.

[12]A virtual currency is a subset of digital currency, which represent all electronic money including that in bank accounts. A virtual currency has been defined by the Financial Crimes Enforcement Network as "a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency. In particular, virtual currency does not have legal tender status in any jurisdiction." Financial Crimes Enforcement Network (2013).

[13]See Jevons (1876).

[14]Financial Crimes Enforcement Network (2013).

[15]Tether is a technology built on top of Bitcoin that allows users to send digital tokens representing US dollars, euros, and yen that are redeemable for fiat currency at Tether Limited in Hong Kong, which holds the currency on a 1-for-1 reserve basis. See Tether (2016).

The bitcoins themselves are stored on a publicly distributed ledger at bitcoin addresses also known as public keys.[16] To send bitcoin, a user needs to know the receiver's public key. Each public key is associated with one or more private keys that are used to "sign" a transaction and transmit the bitcoins.[17] As such, private keys should be kept secret to prevent unauthorized transfer. These private keys are collected and managed via "wallets," which can be held by a wallet service provider, stored on the user's computer, or even written down on paper.[18]

Once the transaction is entered and signed by the sender via a private key, it is broadcast on a public ledger within Bitcoin for verification via a consensus process known as proof-of-work.[19] Consensus is a way to verify that bitcoins or other digital tokens were actually transferred and prevents the same digital tokens from being transferred again by the same sender, a problem known as double spending.[20] Bitcoin's proof-of-work accomplishes this goal by creating a mathematical puzzle that takes time and CPU power to solve.[21] Once submitted to the public ledger, a transaction will be included in a block of other transactions, which will be verified or "mined" by the Bitcoin network by solving the proof-of-work puzzle.[22] Each solved block references the block before it and this creates a blockchain.[23] While it is possible to have multiple blockchains when a miner re-solves a block earlier in the chain, only the longest is recognized as the main and legitimate blockchain and thus verified.[24]

Miners are economically incentivized to continue to build on the longest blockchain. The miner that is first to verify a block is rewarded with bitcoin bounties and transaction fees.[25] Bounties are bitcoins newly created by the protocol and distributed to the miner who was first to solve a block's mathematical puzzle on the longest blockchain.[26] Transaction fees are amounts specified by the sender and

[16]Brito and Castillo (2016), p. 7.

[17]Brito and Castillo (2016), p. 7.

[18]Walsh (2015).

[19]Brito and Castillo (2016), pp. 7–8, 34.

[20]Brito and Castillo (2016), pp. 5–6.

[21]Brito and Castillo (2016), pp. 8–10.

[22]Bitcoin Wiki (2016).

[23]Bitcoin Wiki (2016).

[24]Bitcoin Wiki (2016).

[25]Brito and Castillo (2016), pp. 8–10.

[26]Only the longest blockchain is recognized as legitimate and rewarded. While it is possible to mine a shorter blockchain until it becomes the longest, it is economically inefficient to do so. The chance that a miner solves a particular block is proportional to their CPU relative to the CPU of all other miners. In order to create the longest chain, they would need to consecutively be the first to mine the number of blocks necessary for the shorter chain to overtake the longer. So a miner with 1% of the CPU power could expect .01 reward on average mining the longest chain. They could expect .00002 reward on average for mining a chain one shorter than the longest (.01*.01*2 rewards for 2 blocks). Bitcoin Wiki (2016).

included in a transaction's block.[27] This fee is awarded along with the bounty to a successful miner.[28]

Because of the way blockchain is implemented, it has some features that differentiate it from more traditional payment methods. Two that will be important in the discussion are pseudo-anonymity and multi-signature transactions.

Bitcoin transactions are pseudo-anonymous because every transaction that ever occurred is recorded on a public ledger, while not revealing any personal identity information. The only hint of someone's identity is their public address. Via some analytical techniques, public addresses can be tied to identities,[29] but these are difficult if not impossible to apply to the entire blockchain. Additionally, users can create new addresses for each transaction or employ the services of a tumbler[30] to make it difficult for law enforcement officials to track. Other blockchains have employed techniques to hide the public addresses and the amounts.[31]

Another feature of the Bitcoin protocol is multi-signature transactions. With "multi-sig," a wallet can be set up so that it has multiple private keys and requires more than one of those keys to sign a transaction before it is processed.[32] For example, a common form of feature is the 2-of-3 multi-sig where two of the three private keys need to sign. This feature can be used to enhance the security of wallets. The private keys can be stored on separate devices so there is no single point of failure that a hacker can take advantage of.[33] The hacker would need to compromise at least two devices in order to steal bitcoins.

Multi-sig is also used by anti-fraud service providers such as BitGo. For 2-of-3 multi-sig, a user would control two private keys and the service provider would control the third. The user would sign a transaction and the service provider would review for potential fraud. BitGo also allows enterprise users to set spending limits and treasury policies.[34] If the analysis yields no red flags, then the service provider would sign it using its private key. If the transaction was suspect, the service provider would contact the user and not sign the transaction. The user could request the transaction be signed by the service provider if the transaction was as intended. The user could also override using the second of their keys. The service provider cannot prevent a transaction or initiate one, but can serve as a fraud alert system for the user.

---

[27]Bitcoin Wiki (2016).

[28]Bitcoin Wiki (2016).

[29]Bradbury (2013).

[30]A bitcoin tumbler is a service that takes a user's bitcoins, mixes them with other users' bitcoins, and then redistributes the user's bitcoins to another of the user's accounts. Doing so makes tracking a particular bitcoin transaction through addresses difficult. New York's Department of Financial Services has considered outlawing tumblers due to their potential for money laundering, but also recognize that there may be legitimate uses. See Freifeld (2014).

[31]An example of such an anonymous cryptocurrency is Zcash. See, e.g., Prisco (2016).

[32]See Davenport (2015).

[33]Davenport (2015).

[34]BitGo (2014).

Blockchain technology provides a new payment rail for the transfer of funds that exists outside the traditional financial system. Cryptocurrencies can be transferred over the Internet and these transfers are verified by a decentralized community of miners. The pseudo-anonymous nature of cryptocurrencies like bitcoin and the ability to split control of funds between several users through multi-signature transactions create some interesting opportunities as well as some practical and regulatory problems.

Blockchain technology allows startups to enter the payment space and provide money transfers to consumers. Typical businesses in the space include wallet service providers, which allow users to manage their cryptocurrencies like bank accounts[35] and exchanges, which allow for the trading of cryptocurrencies for other cryptocurrencies or fiat currencies. However, these technology companies remain subject to many of the same vulnerabilities as other financial institutions and few operate in a vacuum without relying on the services of a third-party service provider. The next section will discuss the regulation of these third parties under federal and state law.

4 Regulatory Oversight of Third-Party Service Providers

Financial institutions are overseen by government agencies on the federal and state levels. The type of financial institution determines which laws and regulations apply and what regulatory agencies have supervisory authority. As the laws are not uniform, the extent of this authority also varies. In particular, the authority to regulate and examine third-party service providers depends on the financial institution being serviced. An individual service provider that works with two or more financial institutions may find that it is subject to different authority under each.

This section begins by examining federal regulations' reach to third-party service providers and the reasons behind it. Next, the extent of state regulation over third-party service providers is briefly summarized along with discussion of virtual currency regulation. Finally, this section reviews how states and the Federal Government are cooperating to ease the regulatory costs and the burdens on the financial institutions.

4.1 Federal Regulation

Federal financial law generally applies to third-party service providers through the financial institution they work with. At the federal level, depository institutions are

[35]Either the user or the wallet service provider may have control over these funds depending on the implementation.

overseen principally by one of four regulatory agencies: the Federal Depository Insurance Corporation (FDIC),[36] the Board of Governors of the Federal Reserve System (FRB),[37] the Office of the Comptroller of the Currency (OCC),[38] and the National Credit Union Administration (NCUA).[39] The FDIC, the FRB, and the OCC are together the "appropriate" federal banking agencies.[40] For the purpose of federal consumer financial protection laws, the Consumer Financial Protection Bureau (CFPB) generally has exclusive supervisory authority.[41] However, MSBs, a category of financial institution that most of the virtual currency startups fall under, are not currently subject to oversight by the FDIC, the FRB, the NCUA, or the OCC.[42]

Federal financial laws and regulations advance a number of important goals such as protecting consumer, combating money laundering and terrorist financing, and ensuring the safety and soundness of the financial system. Insured depository institutions may be subject to civil monetary penalties for, *inter alia*, violating laws and statutes, engaging in reckless behavior, or failing in executing their fiduciary duty.[43] Through these penalties, federal regulatory agencies can punish non-compliance and enforce risk management recommendations. MSBs, however, do not have a federal regulatory system to the same extent as other federally-regulated institutions with only AML and consumer protection laws applying to them. The rest of the regulation of MSBs is left to state law. The federal regulatory agencies enforce these laws and regulations through examinations of the financial institutions and their service providers.

This section begins by reviewing the Bank Service Companies Act (BSCA), which first extended regulatory authority to third-party service providers for the appropriate banking agencies. It discusses the reasons and limitations of this extension. Next, the Examination Parity and Year 2000 Readiness for Financial Institutions Act is discussed. This law gave temporary authority to the NCUA to

[36]The FDIC oversees state banks that are not members of the Federal Reserve System and foreign bank branches that it insures as well state savings associations. 12 U.S.C. § 1813 (q).

[37]The FRB oversees Federal Reserve System member state banks, bank holding companies and their subsidiaries, savings and loan holding companies and their subsidiaries, and foreign banks without an FDIC-insured branch as well as additional authority over foreign banks arising from the International Banking Act of 1978. 12 U.S.C. § 1813 (q).

[38]The OCC oversees national banking associations, federal branches and agencies of foreign banks, and federal savings associations. 31 C.F.R. § 1010.100 (ff) (2016).

[39]The NCUA has supervisory authority over federal credit unions. 12 U.S.C. § 1756.

[40]12 U.S.C. § 1813 (q).

[41]The Consumer Financial Protection Bureau oversees insured depository institutions and credit unions as well a non-depository institutions offering consumer financial products. 12 U.S.C. § 5514–16.

[42]The OCC has been considering a federal fintech charter, which would allow some virtual currency businesses to register as special purpose national banks. On 2 December 2016, the OCC opened up the proposed charter to comments. See Office of the Comptroller of the Currency (2016).

[43]12 U.S.C. § 1818 (i); 12 U.S. Code § 1786.

examine credit unions. Its promulgation and sunset give insight into the considerations given to the regulation of third-party service providers. Finally, the reach of AML law is discussed. The regulations span institutions overseen by the FDIC, the FRB, the NCUA, and the OCC as well as granting authority to examine MSBs to the Internal Revenue Service (IRS). Combined with the Bank Service Company Act, these regulations only reach the third-party service providers of the appropriate federal banking agencies.

4.1.1 Bank Service Companies Act

The BSCA was enacted in 1962 and allowed banks to invest in "Bank Service Companies." Advances in automated technology made computerized processing of checks and other clerical services possible and the increase in the number of transactions made it necessary. While many large banks were directly acquiring this technology, small and mid-sized banks did not have the capital do so themselves. Legal limits on proper investments for federal banks prevented them from combining funds with other banks to create bank service companies to acquire this technology. The BSCA aimed to lower these barriers.

However, there was a concern about permiting "banks to avoid the examination and supervision of vital banking functions by the simple expedient of farming out such functions" be it through a bank service company or other third-party.[44] Thus, regulatory authority was extended to all third parties.[45] It must be noted that these "vital banking functions" are limited. Banks had been relying on third parties such as lawyers, accountants, marketing firms, transportation and guard services for a long time and it was thought that federal supervisory agencies would only need to examine or regulate these companies in unusual situations.[46] In order to guide supervisory agencies in administering their responsibilities, Congress specified a non-exhaustive list of permissible bank service company activities in the Act. The modern incarnation includes "check and deposit sorting and posting, computation and posting of interest and other credits and charges, preparation and mailing of checks, statements, notices, and similar items, or any other clerical, bookkeeping, accounting, statistical, or similar functions performed for a depository institution."[47] Thus, while the BSCA seems to extend to any third-party, in practice this authority is limited by the discretion of the appropriate federal supervisory agency.

The BSCA has been amended multiple times and now requires that, regardless of the existence of a contract:

---

[44]H. Rept. No. 2062 (87th Cong. On H. R. 8874, July 30), p. 2.

[45]Bank Service Corporation Act, Pub. L. 87–856, 76 Stat. 1132 (1962), (codified as amended at 12 U.S.C. §§ 1861 et seq.).

[46]S. Rept. No. 2105 (87th Cong. On H. R. 8874, Sept. 18, 1962), p. 3.

[47]12 U.S.C. 1863.

> Whenever a *depository institution* that is regularly examined by an *appropriate Federal banking agency*, or any subsidiary or affiliate of such a *depository institution* that is subject to examination by that agency, causes to be performed for itself, by contract or otherwise, any services authorized under this chapter, whether on or off its premises –
>
> (1) such performance shall be subject to regulation and examination by such agency to the same extent as if such services were being performed by the depository institution itself on its own premises, and
> (2) the depository institution shall notify each such agency of the existence of the service relationship within thirty days after the making of such service contract or the performance of the service, whichever occurs first.[48]

The term depository institution encompasses the more traditional financial institutions such as banks, credit unions and savings associations.[49] Furthermore, it is limited to the financial institutions under the supervision of "the appropriate Federal banking agency," those being the FDIC, the OCC and FRB.[50] These agencies note that, while they have the power to supervise, the bank must also monitor its own service providers.[51]

The financial institutions themselves are expected to ensure that their service providers are compliant with financial regulation via a variety of risk management measures. The existence of the BSCA gives banks more leverage in obtaining access to their service providers' internal information that might not otherwise be garnered by contract negotiation. The OCC emphasizes banks' relationship with their service providers by stating that legal liability may extend to the financial institutions for the acts of their service providers.[52] The OCC lays out a framework for creating a relationship with a third-party including planning, due diligence in the selection, and termination.[53] Financial institutions are expected to continually monitor their service providers and take corrective action when needed.[54] The OCC also instructs that contract negotiation contain compliance provisions and a statement that performance is subject to OCC review.[55]

---

[48]12 U.S.C. 1867 (c) (emphasis added).

[49]The "term 'depository institution' means, except when such term appears in connection with the term 'insured depository institution,' an insured bank, a savings association, a financial institution subject to examination by the appropriate Federal banking agency or the National Credit Union Administration Board, or a financial institution the accounts or deposits of which are insured or guaranteed under State law and are eligible to be insured by the Federal Deposit Insurance Corporation or the National Credit Union Administration Board." 12 USC 1861 (b) (4).

[50]12 U.S. Code § 1813.

[51]Federal Financial Institution Examination Council (2012) (citing 12 U.S.C. §§ 1464 (d) (7) for Federal Savings Association and as well as 1867 (c)); Consumer Financial Protection Bureau (2012) http://files.consumerfinance.gov/f/201204_cfpb_bulletin_service-providers.pdf (citing 12 U.S.C §§ 5514 (c), 5515 (d), and 5516 (c) (these sections in turn refer to 12 U.S.C § 1867 (c)).

[52]U.S. Comptroller of the Currency (2013).

[53]U.S. Comptroller of the Currency (2013).

[54]U.S. Comptroller of the Currency (2013).

[55]U.S. Comptroller of the Currency (2013).

In conclusion, the BSCA provided the "appropriate" federal banking agencies with a broad grant of authority over third-party service providers. This authority is exercised at the discretion of these agencies, but is generally only applied to providers of vital banking functions. The existence of regulatory authority does not lessen the necessity of financial institutions to perform the proper due diligence and monitor their service providers. While the FDIC, the FRB, and the OCC were granted this authority, the NCUA lacked the ability to examine credit union service providers. Shortly before the turn of the millennium, that would change.

4.1.2 Examination Parity and Year 2000 Readiness for Financial Institutions Act

The year 2000 marked the close of the millennium and financial institutions were faced with the Year 2000 or "Y2K" bug. The bug was the result of how most computers recorded dates: two digits for the day, two digits for the month, and two digits for the year.[56] New Years' Day 2000 would send the computers back in time to the year 1900. Programs that depended on relative dates such as those for interest calculation would be thrown into chaos.

Banks and credit unions often relied on third parties for their data processing needs. In anticipation of the Y2K problem, regulatory organizations were hard at work inspecting service providers.[57] The BSCA provided the FDIC, the FRB, and the OCC with the authority to inspect the service providers of the entities under their supervision. However, the NCUA as well as the Office of Thrift Supervision (OTS) lacked this authority. The OTS had been conducting examinations of third-party service providers by requiring savings associations to include this oversight in the contract with their service providers, but this method had resulted in delays, something the rapidly approaching end of the millennium would not allow.[58]

In anticipation of this problem, Congress passed the Examination Parity and Year 2000 Readiness for Financial Institutions Act on 20 March 1998.[59] Along with other provisions meant to address the coming millennium, the Act borrowed language from the BSCA in order to give the NCUA and the OTS examination and regulatory authority over third-party service providers to insured credit unions, credit union organizations, savings associations, and savings and loans entities regardless of the existence of a contract.[60] According to the House Report, the authority that the NCUA wielded was expected to be limited to "those providers to

[56]H. Rept. No. 105–417 (105th Cong. On H.R. 3116 February 24, 1998), p. 5.

[57]H. Rept. No. 105–417 (105th Cong. On H.R. 3116 February 24, 1998), p. 5.

[58]H. Rept. No. 105–417 (105th Cong. On H.R. 3116 February 24, 1998), p. 10.

[59]Examination Parity and Year 2000 Readiness for Financial Institutions Act, Pub. L. 105–164, 112 Stat. 32 (1998).

[60]Pub. L. 105–164.

critical areas that related to the year 2000 computer problem."[61] This authority was only a temporary grant. It was set to and did expire on 31 December 2001, after fear of the Y2K bug had passed.[62]

Since that time, the NCUA has continued to be limited in its ability to address issues of third-party service providers despite recommendations from groups such as the Government Accountability Office (GAO) and the Financial Stability Oversight Council that such authority be granted anew.[63]

Under the Dodd-Frank Act, the OTS powers relating to savings associations were transferred to the OCC, while its powers relating to savings and loans holding companies were transferred to the FRB.[64]

In summary, authority over third-party service providers was extended to the NCUA only by the exigencies of a potential technological disaster. With the passing of the threat, there has not been the political will to renew the law and the NCUA is once again required to negotiate with third-party service providers though credit unions to obtain access to records and facilities.

4.1.3 Application to Anti-Money Laundering Regulation

The Bank Secrecy Act (BSA) was promulgated to require certain institutions to provide disclosures that aid "criminal, tax, or regulatory investigations or proceedings, or in the conduct of intelligence or counterintelligence activities, including analysis, to protect against international terrorism."[65] The law applies to various financial institutions, including those supervised by the FRB, the FDIC, the OCC, and the NCUA. The implementing regulations define and apply to MSBs. This section first outlines the definition of an MSB, specially its application to virtual currency businesses. It then discusses the entities responsible for enforcing AML regulations and how they wield different levels of influence over third-party service providers.

MSBs include dealers in foreign exchange, check cashers, issuers or sellers of traveler's checks, providers of prepaid access, money transmitters, the U.S. Postal Service, and sellers of prepaid access.[66] Virtual currency businesses are often classified as money transmitters as the ambit of the regulations is quite broad. Money transmission services are defined as "the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission "of the

[61]H. Rept. No. 105–417, p. 11.

[62]Examination Parity and Year 2000 Readiness for Financial Institutions Act, Pub. L. 105-164, 112 Stat. 32 (1998).

[63]United States Government Accountability Office (2015); Financial Stability Oversight Council (2016).

[64]Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111–203, 124 Stat. 1376 (2010), § 312.

[65]31 U.S.C. § 5311.

[66]31 C.F.R. § 1010.100 (ff) (2016).

same" to another location or person by any means."[67] By including currency substitutes, the act can be interpreted to reach cryptocurrencies. Furthermore, the geographical reach is likewise extensive. The targeted actors may be a "person wherever located doing business, whether or not on a regular basis or as an organized or licensed business concern, wholly or in substantial part within the United States."[68]

There exist carve outs to this definition including for payment processors and operators of clearance and settlement systems.[69] Assessing whether a particular activity falls within one of these limitations is a fact-based determination.[70] The Financial Crimes Enforcement Network (FinCEN) appears to consider the relationship to regulated financial institutions important. The limitation applicable to payment processors is only available if it is "through a clearance and settlement system."[71] FinCEN has interpreted this to mean only clearance and settlement systems between BSA-regulated institutions.[72] Likewise, operators of these systems are exempt. The regulatory agencies rely on the AML compliance work done by the BSA-regulated institutions to sufficiently mitigate the risk. Virtual currency payment processors do not operate over such a clearance and settlement system so would need to register as MSBs.

Various agencies have regulatory authority relating to AML law. FinCEN has overall "authority for enforcement and compliance" of the regulations implementing the BSA and coordinates with other supervisory agencies.[73] The FDIC, the FRB, the OCC, and the NCUA implement compliance examinations for the financial institutions already within their purview.[74] The IRS is given compliance examination authority over "all financial institutions, except brokers or dealers in securities, mutual funds, futures commission merchants, introducing brokers in commodities, and commodity trading advisors, not currently examined by Federal bank supervisory agencies for soundness and safety." This authority includes MSBs as defined by the implementing regulations.

Third-party service providers are subject to regulatory authority dependent upon the financial institution they do business with. The FDIC, the FRB, and the OCC have authority over all third-party service providers by virtue of the BSCA. The IRS and the NCUA lack this authority over the third-party service providers of MSBs and credit unions. However, one must differentiate between the third-party service providers of MSBs and credit unions. As shown above, a payment processor must register as an MSB and be subject to oversight by the IRS. However,

[67] 31 C.F.R. § 1010.100 (ff) (2016).

[68] 31 C.F.R. § 1010.100 (ff) (2016).

[69] 31 C.F.R. § 1010.100 (ff) (2016).

[70] 31 C.F.R. § 1010.100 (ff) (5) (ii) (2016).

[71] 31 C.F.R. § 1010.100 (ff) (5) (ii) (B) (2016).

[72] Financial Crimes Enforcement Network (2013b). See also Financial Crimes Enforcement Network (2014).

[73] 31 C.F.R. § 1010.810 (a).

[74] 31 C.F.R. § 1010.810 (b).

a payment processor working through a clearance and settlement system between BSA-regulated institutions, like credit unions, need not register as an MSB. Therefore, a payment processor is considered a third-party service provider to a credit union, but cannot be considered a third-party service provider to an MSB.

4.2 State Regulation

States also have a wide range of laws relating to money transmitters targeting money laundering and providing consumer protection as well as advancing other state interests such as maintaining public confidence in financial institutions, market enhancement, and fraud prevention.[75] There is a large amount of duplicative overlap in between States, as no "passporting" system for licensing exists like in Europe.[76] This regime often proves prohibitively costly for young startups without a lot of capital.[77]

In June of 2015, New York State Department of Financial Services published the final Bitlicense rules, a regulatory framework for virtual currency businesses.[78] According to these rules, Virtual Currency Business licensees must allow the superintendent of financial services to examine their financial condition, safety and soundness, management policies, legal compliance, and any other matter that may affect the virtual currency business.[79] Businesses that must register under this framework generally include transmitters, exchangers, deposit holders, brokers, issuers, and administrators of virtual currency.[80] While this examination authority does extend to affiliates, it does not extend to third-party service providers.[81]

In December of 2014, the National Conference of Commissioners on Uniform State Laws' Final Study Committee on Alternative and Mobile Payment Systems released a report urging the commission to form a drafting committee to address virtual currency issues and provide a model framework for state legislatures.[82] Discussion drafts of the Regulation of Virtual Currency Business Act were released in 2015 and 2016, but there is no final draft as of this writing.

The 2016 discussion draft takes care in defining what constitutes virtual currency business activity. The definition focuses on the verbs "exchange, transfer,

[75]Lo (2016), pp. 117–18.

[76]European Banking Authority (2016).

[77]Lo (2016), p. 132 (noting that complying with the five most populous states would require posting of a minimum of $1.2 million in surety bonds).

[78]New York State Department of Financial Services (2015).

[79]23 NYCRR 200.13 (a).

[80]23 NYCRR 200.2 (q).

[81]Affiliates are entities that control or are controlled by the licensee. 23 NYCRR 200.2 (a); 23 NYCRR 200.13 (d).

[82]National Conference of Commissioners on Uniform State Laws (2014).

and store" in connection with virtual currencies.[83] In addition to the virtual currency itself, the regulation also applies to businesses that control enough "credentials" (private keys) to unilaterally transact or prevent transaction of virtual currencies.[84] However, the discussion draft notes that multi-sig is an area where further research and consultation is needed.[85]

Third-party service providers that do not control the requisite number of private keys would not be covered under this framework. The framework specifically excludes entities that contribute "connectivity software or computing power to a decentralized virtual currency," provide "data storage or security services for a virtual currency business and is not otherwise engaged in virtual currency business activity on other persons' behalf."[86] As these third-party service providers would not be required to be licensed under the discussion draft,[87] they would not be required to submit to examination directly. Neither are they required to submit to examination vis-à-vis their relationship with the virtual currency business as examinations are only "of a licensee or any of a licensee's facilities or servers wherever located."[88]

Like under federal law, MSBs' third-party service providers are generally not subject to direct regulation and examination. The lack of authority allows these businesses to grow beyond state borders without worrying about paying compliance costs for duplicative regimes. However, these costs are lessening as federal and state agencies cooperate to regulate MSBs. The question is whether this reduction in cost tips the scales in favor of also regulating third parties.

4.3 Coordinating Examinations Between States and the Federal Government

Given the mix of federal and state regulation and overlapping agency responsibilities, cooperation amongst agencies is imperative to relieve the burden on both government resources and MSBs. To this end, a number of regulatory agency associations and intra-agency agreements have been established.

The Money Transmitter Regulators Association (MTRA) is a non-profit dedicated to establishing a cooperative regulatory framework for MSBs.[89] The membership consists of state regulators from 48 states (excluding Montana and Rhode

[83]National Conference of Commissioners on Uniform State Laws (2016a).
[84]National Conference of Commissioners on Uniform State Laws (2016a), pp. 5–7.
[85]National Conference of Commissioners on Uniform State Laws (2016a), pp. 5–7.
[86]National Conference of Commissioners on Uniform State Laws (2016a), p. 5.
[87]National Conference of Commissioners on Uniform State Laws (2016a), p. 12.
[88]National Conference of Commissioners on Uniform State Laws (2016a), p. 34.
[89]Money Transmitter Regulators Association (2016b).

Island) as well as the District of Columbia and the U.S. Virgin Islands.[90] MTRA issued the Money Transmitter Regulators Cooperative Agreement in 2002[91] and the MTRA Examination Protocol in 2010. The Agreement and Protocol established a framework for coordinating examinations and sharing information.[92]

MTRA partnered with the Conference of State Bank Supervisors (CSBS) and released the Nationwide Cooperative Agreement for MSB Supervision[93] and the Protocol for Performing Multi-State Examinations[94] in January of 2012. The Multi-State MSB Examination Taskforce (MMET) was established to allow states to better coordinate their examination of MSBs and reduce duplicative costs.

The Conference of State Bank Supervisors along with other state financial regulatory organizations have representatives on the State Liaison Committee of the Federal Financial Institutions Examination Council (FFIEC) along with voting rights.[95] The State Liaison Committee allows state agencies to coordinate with their federal counterparts on policy, guidance, and training.[96]

In an effort to improve federal and state cooperation, Congress passed the Money Remittances Improvement Act of 2014 to "allow the Secretary of the Treasury to rely on State examinations for certain financial institutions, and for other purposes."[97] As the Treasury delegates its authority to the appropriate supervising agency through regulation, agencies such as the FDIC, the FRB, the OCC, and the IRS may also rely on state examinations within this delegated authority.

With this cooperation, the federal and state governments reduce the costs to individual regulators as well as the financial institutions supervised. The reduction is especially important to MSBs, which may do business in multiple states and be subject to both federal and state law. The next section discusses whether MSB service providers should also be subject to this regulation and the costs associated with it.

5 Extension of Authority Over MSB Service Providers

As shown in the preceding section, the majority of federal and state financial regulations do not reach MSB service providers. However, MSB service providers still perform vital functions in money transmission. These service providers are

[90]Money Transmitter Regulators Association (2016a).

[91]Money Transmitter Regulators Association (2016c).

[92]Conference of State Bank Supervisors & Money Transmitter Regulators Association (2016), p. 11.

[93]Conference of State Bank Supervisors & Money Transmitter Regulators Association (2012a).

[94]Conference of State Bank Supervisors & Money Transmitter Regulators Association (2012b).

[95]Federal Financial Institutions Examination Council (2016).

[96]See Conference of State Bank Supervisors & Money Transmitter Regulators Association (2016), p. 15.

[97]Money Remittances Improvement Act of 2014, Pub. L. 113–156, 128 Stat. 1829 (2014).

especially important in the nascent virtual currency space as they can offer expertise and standardized infrastructure to an MSB, allowing the MSB to focus on developing its technological value proposition.

On 2 August 2016, Bitfinex, a Hong Kong-based bitcoin exchange, was subject to a security breach that resulted in the theft of 119,756 bitcoins (worth roughly 66 M USD at the time).[98] Scrutiny immediately fell upon BitGo, a third-party service provider of a security platform for the exchange.[99] As 2-of-3 multi-sig security was implemented, BitGo likely needed to approve the transactions before transmission.[100] At the same time, BitGo assured users that "BitGo systems were not breached in this attack and our software functioned correctly."[101] The consulting firm Ledger Labs was hired to investigate. They identified a "key security breach" that allowed large amounts of bitcoins to be released without BitGo being alerted.[102] As of this writing, the investigation continues and the complete details of the breach are not available. Nevertheless, this example serves to illustrate the role of a third-party service provider in the bitcoin space.

BitGo touts itself as a "leading security platform."[103] Together with the CryptoCurrency Certification Consortium (C4), BitGo helped pioneer the CryptoCurrency Security Standard to help improve industry best practices.[104] BitGo subjected itself to external security audits.[105] Its efforts had won industry trust with its security solution being implemented on multiple bitcoin exchanges such Kraken and Bitstamp.[106] Nevertheless, as an MSB service provider, BitGo is not subject to examination or regulation by the financial industry.

The question this section addresses is whether such MSB service providers should be directly supervised by the state and federal regulatory agencies. Section 5.1 discusses how the emergence of virtual currency technology has introduced novel risks. Section 5.2 examines the current means by which regulators and MSBs can address the risks of MSB service providers in general. Section 5.3 argues that, though risks exist, extending supervisory authority over MSB service providers to virtual currency MSBs is likely inadvisable given the current resources available to regulators and the scale of the risk.

[98]Higgins (2016).
[99]Higgins (2016).
[100]Higgins (2016).
[101]Belsh (2016a).
[102]Bitfinex (2016).
[103]Bitgo (2016).
[104]CryptoCurrency Certification Consortium (2015).
[105]Belsh (2016b).
[106]Torpey (2016).

5.1 Risk and Virtual Currency Businesses

The considerations involved with regulatory authority are generally applicable to all MSB service providers. However, advances in virtual currency technology have made money transmission outside of the traditional banking payment rails much easier. Previously, it was simply much more efficient to settle money transfers within the payment rails connected to a trusted third-party, the banking industry.

Now businesses with a modicum of technical expertise could develop software to execute transfers without sending instructions to their bank account provider. Many businesses seized upon the opportunities to realize efficiencies in money transfers by avoiding using another financial institution as a necessary middleman.

Bitcoin allowed bitcoin-denominated transfers to be executed without the need to settle with a bank. A wallet provider or an exchange could send bitcoins without altering their bank account balance. While it is true that fiat currency/virtual currency transactions would affect the account balance of virtual currency wallets and exchanges, it creates a layer of separation that previously did not exist. Once currency was converted to virtual currency within a virtual currency MSB, the account provider could not monitor the business's customer activity without developing the technical skills for blockchain analysis. The size of the virtual currency industry often made investing in these technical skills inefficient for the account provider. The account holder would need to rely completely on reporting by the virtual currency MSB itself.

The lack of transparency naturally made account providers skittish about servicing virtual currency MSBs. Before Bitcoin, these financial institutions could examine an MSB's customer fund transfers, at least obliquely, by monitoring an MSB's bank account activity. As shown above,[107] account providers still remain legally liable for executing proper due diligence and continual monitoring of their account holders. Even if legally compliant, virtual currency MSBs posed reputational risks should they be compromised by hackers.

Enter third-party service providers for virtual currency MSBs. These businesses could provide critical services for MSBs, while not being subject to the same regulation and supervision had the activity been conducted internally. Third-party service providers to financial institutions supervised by the FDIC, the FRB, and the OCC are subject to such regulation and supervision. While it is true that credit union service providers are not subject to this supervision and regulation, their transactions are visible over the traditional payment rails.

[107] See Sect. 4.1.1.

5.2 Mitigating the Risk of MSB Service Providers

Similar to the NCUA, regulatory agencies can attempt to mitigate the risks posed by third-party service providers by using voluntary examinations, participating in examinations by other regulatory agencies with this authority, and indirectly influencing the service providers through an MSB.[108]

Voluntary examinations can and have been refused by third-party service providers in the past according to the GAO Report regarding credit union service providers.[109] Submitting to examinations costs both money, in the form of fees paid to the examiner,[110] and time away from providing the central service. Even when consent is negotiated, it is at the cost of time. These costs effect both the MSB and its service providers. Virtual currency-based businesses may prove especially costly as examination may require a more specialized skill set.

Likewise, permission to participate in examinations by other agencies has also been refused.[111] Allowing an agency without authority to participate in an examination may be seen as duplicative, costly, and against the spirit of existing federal and state cooperation agreements and joint examination organizations such as the Federal Financial Institutions Examination Council and the the Multi-State MSB Examination Taskforce. Furthermore, this approach would only work if there exists another agency with examination authority over the third-party service provider. As discussed above, unless the MSB service provider also does business with a financial entity supervised by the FDIC, the FRB, or the OCC, there is likely no such agency.

A regulator may direct an MSB to have a third-party service provider correct perceived deficiencies with their processes. Contractual duties such as opening books and records to examination and sending reports directly to regulatory agencies can be negotiated between the MSB and the third-party service provider in order to achieve this goal. However, the inability to directly examine the third-party service provider also makes the determination of deficiencies harder. Additionally, MSBs may lack the leverage to influence the third-party service providers. If third-party service providers refuse to make the recommended changes, the regulator can only recommend that the transactional relationship be terminated.

In summary, the existing methods of reducing the risks of third-party service providers have their deficiencies. However, amending existing law to allow for direct regulation and examination may be inadvisable and premature.

---

[108]United States Government Accountability Office (2015), p. 31.

[109]United States Government Accountability Office (2015), p. 31. The National Association of Credit Union Service Organizations is unaware of any situations where examiners have been denied by a credit union service organization. As these organizations are owned by credit unions, this cooperation is unsurprising. National Association of Credit Union Service Organizations (2015).

[110]The existence and extent of examination fees varies by state. The 2016 discussion draft of the Regulation for Virtual Currency Business Act recommends that licensees pay "reasonable costs." National Conference of Commissioners on Uniform State Laws (2016a), p. 34.

[111]United States Government Accountability Office (2015), p. 31.

5.3 Regulatory Authority Should Not Be Extended to MSB Service Providers

In order to evaluate whether regulatory authority should be extended to MSB service providers, it is useful to compare them with credit union service providers. As shown above, credit union service providers are not subject to the regulatory authority of the NCUA at this time. Credit union service providers were temporarily under this authority from 1998 to 2001 and it has been recommended that this authority be renewed by the Government Accountability Office and the Financial Stability Oversight Council. However, even under the assumption that this approach is appropriate for credit union service providers, subjecting MSB service providers to similar regulatory authority is inadvisable because of differences in the regulatory framework surrounding MSBs and their relative risk profile. The argument still holds for virtual currency MSBs despite their increased risk relative to other MSBs as outlined in Sect. 5.1.

Both federal and state laws would need to be amended to extend existing authority over MSBs to their service providers. Revision at the federal level would allow the IRS to examine these service providers for AML law compliance. The GAO Report recommended the extension of examination authority to the NCUA over credit union service providers. However, one must differentiate the risk posed by a third-party service provider to credit unions and those to MSBs. Any service that would have control over or allow the transmission of customer funds would fit the definition of an MSB on the federal level subjecting it to regulation and examination. These types of service providers would not be subject to NCUA examination. Thus, the AML risk posed by MSB service providers is less than credit union service providers as MSB service providers do not have control over customer funds. As it is the MSB that does have control over the customer funds, they are best suited to follow the registration and recordkeeping requirements.

The pseudo-anonymous nature of some blockchain technology does introduce an interesting capability in the pursuit of AML compliance. Wallets and exchanges such Coinbase can track how bitcoins are spent on the public ledger even after the bitcoins are transferred out of the control of said wallets and exchanges.[112] Questions over the right to privacy aside, the existence of the public ledger also makes it easier for certain AML compliance functions to be outsourced to companies specializing in analyzing the blockchain such as Chainanalysis. Doing so creates economies of scale as a single company has access to the complete record of all transactions. As these companies are already performing ongoing monitoring of the blockchain, onboarding new MSBs requires little additional analysis.

These third-party service providers need not be subject to regulatory authority as their services are inherently tied to fulfilling compliance needs. They are already

[112]Coinbase users have complained that their accounts were banned after allegedly transferring bitcoins to bitcoin addresses connected to gambling and illegal drugs. See Caraluzzo (2014).

influenced by the threat of termination and the reputational damage that comes from failing to properly provide their core service.

Other regulatory goals are advanced by state governments. Individual states can pass statutes and regulations, but adopting a uniform framework is more efficient. However, from a practical standpoint, a uniform framework is hard to implement, as it would need to be adopted by each individual state and territory. By way of comparison, the Uniform Money Services Act is a model framework promulgated by the National Conference of Commissioners on Uniform State Laws in 2000 with the intent to improve AML regulation.[113] Since then, only seven states and two U.S. territories have adopted this model framework.[114] Slow adoption means that states will not be able to take full advantage of the joint examination framework established between federal and state regulatory agencies.

Each state agency would need to build its own resources to examine MSB service providers in the initial stage. The NCUA offers centralized oversight for credit unions allowing it to develop the resources and technical skills necessary for its mission and to benefit from the economies of standardization.[115] Though multi-state examination has come a long way in easing the burden on individual state regulatory agencies, each must have its own staff capable of conducting individual examinations. The examination of virtual currency MSBs alone necessitates a certain degree of technical skill. To extend examination authority over MSB service providers would tax the existing system.

Furthermore, the industry would push back against this extension of authority. Associations representing both the credits unions and service providers opposed the extension of NCUA authority.[116] The virtual currency space has likewise been slow to accept regulatory authority.[117]

For virtual currency MSB service providers, it comes down to a matter of industry risk profile. There is also a major difference in the size and risk posed by virtual currency businesses when compared with credit unions. At the end of 2015, credit unions had assets of over $1,191 billion in the United States.[118] Compare this amount to the just over $12 billion market capitalization of all virtual currencies worldwide listed on CoinMarketCap as of this writing.[119] The costs outlined above in developing the resources necessary to properly examine these virtual currency MSB service providers would likely overburden the development of this ecosystem.

[113]National Conference of Commissioners on Uniform State Laws (2016b).

[114]National Conference of Commissioners on Uniform State Laws (2016b).

[115]In order to address cyber threats, the NCUA has around 50 IT examiners and specialists. United States Government Accountability Office (2015), p. 25.

[116]CUToday (2015).

[117]For example, many companies chose to cut off ties with New York instead of subjecting themselves to the state's virtual currency licensing scheme. See Roberts (2015).

[118]Credit Union National Association (2016).

[119]CoinMarketCap (2016).

Because of the above practical considerations of regulating MSB service providers, it is better that they be governed by private contractual law with their MSBs. However, just because these entities are excluded from regulation does not mean that MSBs should be free to outsource these functions and not be held responsible if they are executed in ways that are not compliant with existing laws. The MSBs themselves should be held liable for the malfeasance of their agents and should be circumspect in choosing their partners.

6 Conclusion

MSB service providers form a unique gap in the regulatory framework governing our financial system. The MSBs they service rely on them for a range of functions, some critical to the financial institutions. While it is tempting to close this gap to be more in line with the federal regulation of existing financial institutions, the fractious nature of MSBs' regulatory authority shared between federal and state governments makes this extension impractical. Private law may substitute for regulatory authority over MSB service providers to some extent and serves as an economically reasonable alternative to regulations for this niche market.

Acknowledgements I would like to thank Marcelo Corrales, Prof. Mark Fenwick, Jessica Jackson-McLain, Andrea Martínez and Ray Nothnagel for their help and advice in writing this chapter.

References

Belsh M (2016a) Bitfinex breach update. https://blog.bitgo.com/bitfinex-breach-update/. Accessed 13 Oct 2016

Belsh M (2016b) Recent BitGo service improvements. https://blog.bitgo.com/recent-bitgo-service-improvements/. Accessed 13 Oct 2016

Bitcoin Wiki (2016) How bitcoin works. https://en.bitcoin.it/wiki/How_bitcoin_works. Accessed 13 Oct 2016

Bitfinex (2016) Interim update. https://www.bitfinex.com/posts/135. Accessed 13 Oct 2016

BitGo (2014) BitGo launches multi-signature bitcoin security solutions for the enterprise. https://blog.bitgo.com/bitgo-launches-multi-signature-bitcoin-security-solutions-for-the-enterprise/. Accessed 13 Oct 2016

Bitgo (2016) About BitGo Inc. https://www.bitgo.com/about. Accessed 13 Oct 2016

Bradbury D (2013) How anonymous is bitcoin? http://www.coindesk.com/how-anonymous-is-bitcoin/. Accessed 13 Oct 2016

Brito J, Castillo A (2016) Bitcoin: a primer for policymakers. https://www.mercatus.org/system/files/GMU_Bitcoin_042516_WEBv2_0.pdf. Accessed 16 Oct 2016

Caraluzzo C (2014) Coinbase is tracking how users spend their bitcoins. https://cointelegraph.com/news/coinbase-is-tracking-how-users-spend-their-bitcoins. Accessed 7 Nov 2016

CoinMarketCap (2016) Crypto-currency market capitalizations. https://coinmarketcap.com/all/views/all/. Accessed 13 Oct 2016

Conference of State Bank Supervisors & Money Transmitter Regulators Association (2016) The state of state money services businesses regulation & supervision. https://www.csbs.org/regulatory/Cooperative-Agreements/Documents/State%20of%20State%20MSB%20Regulation%20and%20Supervision.pdf. Accessed 13 Oct 2016

Conference of State Bank Supervisors & Money Transmitter Regulators Association (2012a) The enhanced CSBS/MTRA nationwide cooperative agreement for MSB supervision. http://www.mtraweb.org/wp-content/uploads/2012/10/Nationwide-Cooperative-Agreement-for-MSB-Supervision-2012.pdf. Accessed 13 Oct 2016

Conference of State Bank Supervisors & Money Transmitter Regulators Association (2012b) Protocol for performing multi-state examinations. http://www.mtraweb.org/wp-content/uploads/2012/10/Protocol-for-Performing-Multi-State-Exams-01-2012.pdf. Accessed 13 Oct 2016

Consumer Financial Protection Bureau (2012) CFPB bulletin 2012–03. http://files.consumerfinance.gov/f/201204_cfpb_bulletin_service-providers.pdf. Accessed 13 Oct 2016

Credit Union National Association (2016) Credit union report year-end 2015. http://www.cuna.org/uploadedFiles/CUNA/Research_And_Strategy/DownLoads/curepd15.pdf. Accessed 13 Oct 2016

CryptoCurrency Certification Consortium (2015) Introducing the CryptoCurrency Security Standard. http://blog.cryptoconsortium.org/ccss/. Accessed 13 Oct 2016

CUtoday (2015) Senate amendment would give NCUA authority over third-party vendors; Trades Object. http://www.cutoday.info/Fresh-Today/Senate-Amendment-Would-Give-NCUA-Authority-Over-Third-Party-Vendors-Trades-Object. Accessed 13 Oct 2016

Davenport B (2015) What is multi-sig, and what can it do? http://coincenter.org/entry/what-is-multi-sig-and-what-can-it-do. Accessed 13 Oct 2016

Depository Trust & Clearing Corporation (2016) Embracing disruption: tapping the potential of distributed ledgers to improve the post-trade landscape. http://www.dtcc.com/news/2016/january/25/blockchain. Accessed 13 Oct 2016

El-Hindi J (2016) Remarks to the CSBS state federal supervisory forum. https://www.fincen.gov/news/speeches/prepared-remarks-fincen-deputydirector-jamal-el-hindi-delivered-csbs-state-federal. Accessed 17 Oct 2016

European Banking Authority (2016) Passporting and supervision of branches. https://www.eba.europa.eu/regulation-and-policy/passporting-andsupervision-of-branches. Accessed 13 Oct 2016

Federal Financial Institutions Examination Council (2014) Bank secrecy act/anti-money laundering examination manual. https://www.ffiec.gov/bsa_aml_infobase/documents/BSA_AML_Man_2014_v2.pdf. Accessed 7 Nov 2016

Federal Financial Institutions Examination Council (2016) Federal Financial Institutions Examination Council. https://www.ffiec.gov/default.htm. Accessed 13 Oct 2016

Federal Financial Institution Examination Council (2012) Supervision of technology service providers. http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_SupervisionofTechnologyServiceProviders(TSP).pdf. Accessed 13 Oct 2016

Financial Crimes Enforcement Network (2013) FIN-2013-R002: whether a company that offers a payment mechanism based on payable-through drafts to its commercial customers is a money transmitter. https://www.fincen.gov/sites/default/files/administrative_ruling/FIN-2013-R002.pdf. Accessed 13 Oct 2016

Financial Crimes Enforcement Network (2014) Request for administrative ruling on the application of FinCEN's regulations to a virtual currency payment system. https://www.fincen.gov/resources/statutes-regulations/administrative-rulings/request-administrative-ruling-application. Accessed 13 Oct 2016

Financial Stability Oversight Council (2016) FSOC 2016 annual report. https://www.treasury.gov/initiatives/fsoc/studies-reports/Documents/FSOC%202016%20Annual%20Report.pdf. Accessed 13 October 2016

Freifeld K (2014) New York regulator moving ahead on bitcoin regulation. http://www.reuters.com/article/2014/02/11/usa-bitcoin-idUSL2N0LG1P520140211. Accessed 13 Oct 2016

Higgins S (2016) The bitfinex bitcoin hack: what we know (and don't know). http://www.coindesk.com/bitfinex-bitcoin-hack-know-dont-know/. Accessed 13 Oct 2016

Jevons W (1876) Money and the mechanism of exchange. D. Appleton and Co., New York
Kendall G (2015) Kynetix launch commodities blockchain consortium. http://www.kynetix.com/2015/11/23/kynetix-launch-commodities-blockchain-consortium/. Accessed 13 Oct 2016
Lo B (2016) Fatal fragments: the effect of money transmission regulation on payment innovation, 18 Yale J.L. & Tech. 111
Maltese M (2015) Uproov: blockchain timestamping goes professional, notary offices decline begins. https://cointelegraph.com/news/uproov-blockchain-timestamping-goes-professional-notary-offices-decline-begins. Accessed 13 Oct 2016
Money Transmitter Regulators Association (2016a) Members. http://www.mtraweb.org/about/members/. Accessed 13 Oct 2016
Money Transmitter Regulators Association (2016b) money transmitter regulators association. http://www.mtraweb.org/. Accessed 13 Oct 2016
Money Transmitter Regulators Association (2016c) MTRA cooperative agreement. http://www.mtraweb.org/about/cooperative-agreement/. Accessed 13 Oct 2016
National Association of Credit Union Service Organizations (2015) NACUSO letter to Mitch McConnell and Harry Read. https://www.nacuso.org/wp-content/uploads/2015/08/NACUSO-Letter-to-Congress-8-5-15.pdf. Accessed 13 Oct 2016
National Conference of Commissioners on Uniform State Laws (2014) Final study committee on alternative and mobile payments report. http://www.uniformlaws.org/shared/docs/regulation%20of%20virtual%20currencies/2015AM_RegVirtualCurrencies_StudyCmteRpt_2014dec19.pdf. Accessed 13 Oct 2016
National Conference of Commissioners on Uniform State Laws (2016a) 2016 Discussion draft of the regulation of virtual currency business act. http://www.uniformlaws.org/shared/docs/regulation%20of%20virtual%20currencies/2016AM_VirtualCurrencyBusinesses_Draft.pdf. Accessed 13 Oct 2016
National Conference of Commissioners on Uniform State Laws (2016b) Legislative fact sheet—money services act. http://www.uniformlaws.org/LegislativeFactSheet.aspx?title=Money%20Services%20Act. Accessed 7 Nov 2016
New York State Department of Financial Services (2015) Final BitLicense regulation. http://www.dfs.ny.gov/legal/regulations/bitlicense_reg_framework.htm. Accessed 13 Oct 2016
Office of the Comptroller of the Currency (2016) OCC to consider fintech charter applications, seeks comment. https://www.occ.gov/news-issuances/news-releases/2016/nr-occ-2016-152.html. Accessed 16 Feb 2016
Prisco G (2016) Zcash creator on the upcoming Zcash launch, privacy and the unfinished internet revolution. https://bitcoinmagazine.com/articles/zcash-creator-on-the-upcoming-zcash-launch-privacy-and-the-unfinished-internet-revolution-1472568389. Accessed 13 Oct 2016
Roberts D (2015) Behind the "exodus" of bitcoin startups from New York. http://fortune.com/2015/08/14/bitcoin-startups-leave-new-york-bitlicense/. Accessed 13 Oct 2016
Society for Worldwide Interbank Financial Telecommunications (2016) SWIFT on distributed ledger technologies. https://www.swift.com/insights/press-releases/swift-and-accenture-outline-path-to-distributed-ledger-technology-adoption-within-financial-services. Accessed 13 Oct 2016
Tasca P, Liu S, Hayes A (2016) The evolution of the bitcoin economy: extracting and analyzing the network of payment relationships. http://ssrn.com/abstract=2808762. Accessed 12 Oct 2016
Tether (2016) Tether: fiat currencies on the bitcoin blockchain, https://tether.to/wp-content/uploads/2015/04/Tether-White-Paper.pdf. Accessed 13 Oct 2016
Torpey K (2016) After the bitfinex hack, here's why bitstamp is sticking with BitGo. https://bitcoinmagazine.com/articles/after-the-bitfinex-hack-here-s-why-bitstamp-is-sticking-with-bitgo-1470669567. Accessed 13 Oct 2016
U.S. Comptroller of the Currency (2013) OCC 2013-29: third-party relationships. https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html. Accessed 12 Oct 2016
United States Government Accountability Office (2015) Bank and other depository regulators need better data analytics and depository institutions want more useable threat information. http://www.gao.gov/assets/680/671105.pdf. Accessed 13 Oct 2016

Vallabhaneni P, Fauvre D, Shipe A (2016) Overcoming obstacles to banking virtual currency businesses, coin center. http://www.arnoldporter.com/~/media/files/perspectives/publications/2016/05/overcoming-obstacles-to-banking-virtual-currency-businesses.pdf. Accessed 13 Oct 2016

Wadhwa T (2016) We could be set for a 'brave new world' of stock trading. Business Insider. http://www.businessinsider.com/asx-pioneers-blockchain-technology-2016-6. Accessed 13 Oct 2016

Walsh D (2015) Bitcoin wallets explained: how to choose the best wallet for you. http://cryptorials.io/bitcoin-wallets-explained-how-to-choose-the-best-wallet-for-you/. Accessed 16 Oct 2016

Index

M. Corrales et al. (eds.), *New Technology, Big Data and the Law*,
Perspectives in Law, Business and Innovation, DOI 10.1007/978-981-10-5038-1