

**BIG DATA: IP, OWNERSHIP, AND PROTECTION**  
**– AN ANALYSIS**

*Dissertation submitted in part fulfilment for the requirement of the  
Degree of*

**LL.M.**

**Submitted By**

**S. MUHAMMAD ALIKHAN**

**Register No: LM0220004**

**Supervised By**

**Dr. ANIL R. NAIR**



**The National University of Advanced Legal Studies**

**Kochi**

**2020**

## DECLARATION BY THE CANDIDATE

I declare that this dissertation titled “**Big Data: IP, Ownership, and Protection – An Analysis**” submitted at the **National University of Advanced Legal Studies**, in partial fulfilment of the requirement for the award of Degree of Master of Laws in International Trade Law carried out under the supervision of **Dr. Anil R. Nair, Associate Professor (Law), National University of Advanced Legal Studies** has been composed solely by myself and that it has not been submitted, in whole or in part, in any previous application for a degree, except where states otherwise by reference or acknowledgement, the work presented is entirely my own.

Place: Ernakulam

Signature:

Date: 11/10/2021

**S. MUHAMMAD ALIKHAN**

Reg No: LM0220004

International Trade Law

NUALS, Kochi

## **CERTIFICATE OF SUPERVISOR**

This is to certify that S. MUHAMMAD ALIKHAN, Reg. No: LM0220004 has submitted his Dissertation titled, “Big Data: IP, Ownership, and Protection – An Analysis” in partial fulfilment of the requirement for the award of Degree of Master of Laws in International Trade Law to The National University of Advanced Legal Studies, Kochi under my guidance and supervision. It is also affirmed that the dissertation submitted by her is bonafide and genuine.

Place: Ernakulam

Date: 11/10/2021

Signature:

**Dr. Anil R. Nair**

Associate Professor (Law)

NUALS, Kochi

## **ACKNOWLEDGEMENT**

I would like to express my wholehearted thanks to Dr Anil R. Nair. I would like to express my most profound appreciation for helping and guiding me in realizing my dream. I am indebted to him for his encouragement and support throughout the study. He has constantly encouraged me to believe in my work and pushed me to finish the dissertation. He constantly ensured that I stayed on track and generously supported me with invariable information that aided in completing the dissertation. Without his supervision and constant assistance, this project would not have been possible.

My sincere thanks also go to Vice-Chancellor Prof. (Dr.) K.C. Sunny and the other faculty members at the National University of Advanced Legal Studies for their constant guidance and unflinching support.

I want to extend my sincere thanks to the University Library department for providing us with continuous access to online resources and the enriched library of the National University of Advanced Legal Studies, which proved invaluable in helping me complete my dissertation.

I am incredibly thankful to my parents, family members, and friends for their moral support and encouragement, enabling me to complete my dissertation successfully.

I would like to convey my heartfelt gratitude to everyone who supported me in this endeavour.

**S. MUHAMMAD ALIKHAN**

## LIST OF ACRONYMS AND ABBREVIATIONS

&	And
APEC	Asia Pacific Economic Cooperation
Art.	Article
BDVC	Big Data Value Chain
CAC	Cyberspace Administration of China
CII	Critical Information Infrastructure
CIIO	Critical Information Infrastructure Operators
CJEU	European Union Court of Justice
Dr.	Doctor
DVC	Data Value Chain
ECIPE	European Centre for International Political Economy
EEA	European Economic Area
Ed.	Editor
Etc.	Et Cetera (other things)
EU	European Union
FTC	Federal Trade Commission
GB	Gigabyte
Govt.	Government
i.e.	that is
IBM	International Business Machines Corporation
IDC	International Data Corporation
IoT	Internet of Things
IP	Intellectual Property
ISO	International Organization for Standardization
ML	Machine Learning
MNE	Multinational Enterprise
NoSQL	Not Only SQL
OECD	Organisation for Economic Co-operation and Development
PB	Pettabyte
PRC	People's Republic of China

SC	Supreme Court
SCC	Standard Contractual Clause
Sec.	Section
SQL	Structured Query Language
TB	Terrabyte
TDM	Text and Data Mining
UK	United Kingdom
UNCITRAL	United Nations Commission On International Trade Law
US	United States
USITC	United States International Trade Commission
v.	versus
WIPO	World Intellectual Property Organisation
WTO	World Trade Organisation
ZB	Zettabyte

## **TABLE OF STATUES**

### **ASIA PACIFIC ECONOMIC COOPERATION:**

- APEC Privacy Framework

### **EUROPEAN UNION:**

- The Directive on the Legal Protection of Databases (Directive 96/9/EC), 1996
- The Directive on the Protection of Trade Secrets (Directive 2016/943), 2016
- The General Data Protection Regulation (Regulation 2016/679), 2018

### **INDIA:**

- Personal Data Protection Bill, 2009

### **ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT:**

- OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980

### **PEOPLE'S REPUBLIC OF CHINA:**

- Cybersecurity Law of the People's Republic of China, 2017
- Data Security Law of the People's Republic of China, 2021
- Personal Information Protection Law of the People's Republic of China, 2021

### **RUSSIA**

- Federal Law No. 242-FZ of July 21, 2014 on Amending Some Legislative Acts of the Russian Federation in as Much as It Concerns Updating the Procedure for Personal Data Processing in Information-Telecommunication Networks (with Amendments and Additions

### **UNITED STATES:**

- California Consumer Privacy Act of 2018
- Copyright Law of the United States (Title 17) and Related Laws Contained in Title 17 of the United States Code
- Database Investment and Intellectual Property Antipiracy Act of 1996
- Defend Trade Secrets Act of 2016

**WORLD INTELLECTUAL PROPERTY ORGANISATION:**

- Berne Convention for the Protection of Literary and Artistic Works, 1886
- WIPO Copyright Treaty, 1996

**WORLD TRADE ORGANISATION:**

- General Agreement on Trade in Services, 1995
- The Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPs Agreement), 1995



## LIST OF CASES

- *Applied Innovations, Inc. v. Regents of Univ. of Minn.*, 876 F.2d 626, 634-35 (8th. Cir. 1989)
- *Case C-203/02 British Horseracing Board v. William Hill Organization* [2004] ECR I-10415 (ECJ)
- *Case C-338/02 Fixtures Marketing Ltd v. Svenska Spel AB, Fixtures* [2004] ECR I-10497 (ECJ)
- *Case C-362/14, Maximillian Schrems v Data Protection Commissioner*, 2015 EUR-Lex 62014CJ0362 (Oct. 6, 2015).
- *Case C-444/02 Fixtures Marketing Ltd v. Organismos prognostikon agonon podosfairou AE (OPAP)* [2004] ECR I-10549
- *Case C-46/02 Fixtures Marketing Ltd v. Oy Veikkaus Ab* [2004] ECR I-10396 (ECJ)
- CJEU, *C-311/18, Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems*, ECLI:EU:C:2020:559 (Schrems II)
- *Dow Jones & Company, Inc., v. Board of Trade of the City of Chicago* 546 F. Supp. 113 (1982)
- *Feist Publications, Inc. v. Rural Telephone Service Co., Inc.*, 499 U.S. 340, 111 S. Ct. 1282 (1991)
- *Hutchinson v. Fronteer*, 770 F.2d 128 (1985) (8th. Cir. 1989)
- *List Pub. Co. v. Keller*, 30 F. 772 (1887)
- *Zee Telefilms Ltd. v. Sundial. Communications Pvt. Ltd.*, 2003 (27) PTC 457 (Bom)

## TABLE OF CONTENTS

<u>Declaration by the Candidate</u>	<u>I</u>
<u>Certificate of Supervisor</u>	<u>II</u>
<u>Acknowledgement</u>	<u>III</u>
<u>List of Acronyms and Abbreviations</u>	<u>IV</u>
<u>Table of Statutes</u>	<u>VI</u>
<u>List of Cases</u>	<u>VIII</u>
<b>CHAPTER I – INTRODUCTION</b>	<b>1-5</b>
<u>1.1 Background</u>	<u>1</u>
<u>1.2 Statement of Problem</u>	<u>2</u>
<u>1.3 Hypothesis</u>	<u>2</u>
<u>1.4 Research Questions</u>	<u>2</u>
<u>1.5 Research Objectives</u>	<u>3</u>
<u>1.6 Research Methodology</u>	<u>3</u>
<u>1.7 Scheme of the Research</u>	<u>3</u>
<b>CHAPTER II - BIG DATA: WHAT IT IS AND WHY IT MATTERS</b>	<b>6-21</b>
<u>2.1 Introduction</u>	<u>6</u>
<u>2.2 What is Big Data</u>	<u>8</u>
<u>2.3 Characteristics of Big Data</u>	<u>10</u>
<u>2.4 Sources of Big Data</u>	<u>11</u>
<u>2.5 How Big Data Differs from Traditional Data</u>	<u>13</u>
<u>2.6 Big Data Value Creation</u>	<u>14</u>
<u>2.7 Why Big Data Matters</u>	<u>15</u>
<u>2.8 How Big Data Creates Value</u>	<u>16</u>
<u>2.9 Challenges posed by Big Data to Privacy</u>	<u>18</u>
<u>2.10 Conclusion</u>	<u>20</u>
<b>CHAPTER III - BIG DATA AND INTELLECTUAL PROPERTY RIGHTS</b>	<b>22-34</b>
<u>3.1 Introduction</u>	<u>22</u>
<u>3.2 Intellectual Property Rights Concerning Data</u>	<u>22</u>

3.1.1	<u>Copyright</u>	23
3.1.2	<u>Sui Generis Protection</u>	27
3.1.3	<u>Trade Secrets</u>	30
3.3	<u>Conclusion</u>	33

## **CHAPTER IV - OWNERSHIP OF BIG DATA** **35-49**

4.1	<u>Introduction</u>	35
4.2	<u>Defining Personal, Non-Personal Data, and Machine-Generated Data</u>	36
4.3	<u>Property Rights in Data</u>	38
4.4	<u>Data Ownership and Control over Data</u>	39
4.5	<u>Multiple Stakeholders in Data</u>	44
4.6	<u>Consequences Of Data Ownership</u>	47
4.7	<u>Conclusion</u>	48

## **CHAPTER V - PROTECTION OF DATA IN CONNECTION WITH CROSS BORDER DATA TRANSFERS** **50-74**

5.1	<u>Introduction</u>	50
5.2	<u>International and National Legal Frameworks concerning Data Protection and Cross Border Data Transfers</u>	53
5.2.1	<u>Organization for Economic Cooperation and Development</u>	53
5.2.2	<u>Asia-Pacific Economic Cooperation</u>	54
5.2.3	<u>European Union</u>	56
5.2.4	<u>United States</u>	61
5.2.5	<u>People's Republic of China</u>	64
5.2.6	<u>India</u>	68
5.2.7	<u>General Agreement on Trade in Services</u>	69
5.3	<u>Analysis</u>	69

## **CHAPTER VI - CONCLUSION AND SUGGESTIONS** **75-80**

	<u>Bibliography</u>	81
--	---------------------	----

# **CHAPTER I:**

## **INTRODUCTION**

### **1.1 BACKGROUND**

Data is often regarded to be the new oil. Big data has a significant role in today's economy as it is the building block of the new digital economy. Big data is data with a greater variety of increasing volumes and ever-higher velocity. The volume of data generated has seen incredible growth in recent years. There are many legal and ethical quandaries in data dealing that range from privacy, personal security, processing, personal data protection to ownership and control over the data.

Intellectual property rights are the rights that are the result of creativity and that grant the holders a monopoly on the use of that creation for a specified period and are subject to certain exceptions. The underlying aim of granting such a monopoly is to incentivize creators to share their creations with the public and achieve the social benefits of increased creative activity. In light of these elements, it cannot be excluded that certain elements of the big data lifecycle fall within the scope of protection of certain intellectual property rights. Given data's creative nature, economic value, and other inherent values, the critical question remains whether data can be protected as intellectual property.

The ownership and control of data for commercial and internal purposes is an inflection point for organizations, their customers, and the public. Intellectual property and other legal mechanisms for asserting or claiming ownership of data are also being questioned. The data value cycle, which can be rather complicated and involves numerous stakeholders, further complicates data ownership issues. This makes it more challenging to determine who could or would be entitled to claim data ownership. Many such stakeholders may attempt to claim ownership of data by, for example, creating or generating data, or by using, compiling, selecting, structuring, re-formatting, enriching, analyzing the purchase, licensing, or adding value to the data. Accordingly, different stakeholders will have different powers depending on their specific roles in many

instances. No single data stakeholder will, therefore, have exclusive rights. It gets intricate when the individual's right to control the use of his data comes up.

Today's trade is inextricably linked to the cross-border movement of data, either as part of the transaction or as the product itself. The information economy enables the cross-border movement of large amounts of digitized information and data. The interfaces between trade and privacy protection have grown and intensified as data's role in society has grown and intensified, raising critical questions about how to design an appropriate regulatory framework that balances economic and non-economic concerns, as well as national and international interests. The lack of privacy and data protection legislation, as well as divergent approaches among countries that do have such legislation, jeopardize fundamental rights, adequate cross-border data flows, and information freedom. Both the free flow of information across borders and the rights of data subjects must be protected.

## **1.2 STATEMENT OF PROBLEM**

The research paper aims to analyze the application of the intellectual property to big data, the ownership of big data, and the protection and regulation of data in cross-border data transfers.

## **1.3 HYPOTHESIS**

- The existing intellectual property framework is insufficient to accommodate the data economy's current advancements.
- There should be a paradigm shift in how ownership and big data trading issues are addressed.
- Regulation and protection of data in the context of international data transfers require a global policy.

## **1.4 RESEARCH QUESTIONS**

- Whether Big Data can be protected under Intellectual Property Rights?
- Who holds the ownership rights in data?
- How can data be protected in relation to cross-border data transfers?

## **1.5 RESEARCH OBJECTIVES**

The main objectives of this research are:

- To examine the relation between big data and intellectual property.
- To examine the legal and ethical concerns relating to the ownership of big data.
- To analyze the current status of legal frameworks to protect and regulate cross-border data transfer big data.
- To provide suggestions and modifications to that are to be made in the current legal frameworks concerning data protection and cross-border data transfer.

## **1.6 RESEARCH METHODOLOGY**

The study is purely doctrinal or non-empirical. The data collected is both primary and secondary. Legislations and case laws will be used as primary sources to understand the concepts of intellectual property rights, ownership, and data protection and regulation, while journal articles, books, and reports published by various committees and organizations will be used as secondary sources. The collected data is summarised and interpreted in accordance with the research problem's requirements. The inferential method of study shall be used.

## **1.7 SCHEME OF THE RESEARCH**

The following is the chapter structure of the research paper:

1. Introduction
2. Big Data: What it is and why it is important
3. Big Data and Intellectual Property Rights

4. Ownership of Data
5. Protection of Data in connection with Cross Border Data Transfers
6. Conclusions and Suggestions

In the present work, the following scheme of research has been used:

The second chapter, titled 'Big Data: What It Is and Why It Is Important,' delves into the definition and application of big data. The chapter discusses the various definitions for the term "big data." the characteristics of big data have been discussed. There have been distinctions made between big data and traditional data. It has been examined why big data is important to individuals, organizations, and governments. The Big Data Value Chain has been described to aid in comprehension of the process and the numerous stages that data must pass through before it can be used. It has been demonstrated how big data generates value from the perspective of business organizations. Additionally, the privacy concerns raised by big data have been investigated.

The third chapter, titled 'Big Data and Intellectual Property Rights,' examines the application of intellectual property rights to big data. Copyright, Sui Generis Database Rights, and Trade Secrets have been examined, as they are primarily associated with data. The criteria for granting intellectual property protection are analyzed to determine their applicability to big data.

The fourth chapter, titled 'Ownership of Data', analyses the legal and ethical implications of granting ownership rights in data. Personal, Non-Personal, and Machine-generated data have been defined. The concepts of property rights and ownership are examined and contrasted. The rationale behind the want for ownership of data has been examined. Various parties with interest in the data are examined. This is for the purpose of determining who is to be granted access to/rights to data. The ramifications of granting data ownership rights have been examined.

The fifth chapter, titled 'Protection of Data in connection with Cross Border Data Transfers,' initially studies the current data protection and regulation legislations of various jurisdictions in relation to cross-border data transfers. The purpose for doing the same is the determinations of the best practices that are followed there and to take

into account the practical issues of the current data protection regimes. The need for a convergence of data protection regimes has been examined.

Finally, the researcher has concluded the current issues surrounding the application of intellectual property rights to big data, granting ownership rights over data, and data protection in relation to cross-border data transfers. Suggestions have been made to ensure adequate data protection while allowing for the free flow of information across borders.



## CHAPTER II:

### BIG DATA: WHAT IT IS AND WHY IT IS IMPORTANT

#### 2.1 INTRODUCTION

The world is facing a revolution in data. Previously, only a small amount of analogue data was generated and distributed via a limited number of channels. Today, in the Digital Age, a massive amount of data is generated and transmitted on a daily basis from a variety of sources via a variety of channels. “The amount of data stored annually increased to 161 exabytes, up from only 5 exabytes in 2003, roughly equal to the amount of data stored in 37,000 libraries the size of the United States Library of Congress.”<sup>1</sup>

Data is ubiquitous and pervades nearly every aspect of human life. Individuals can create/author data, or machines/sensors can generate it. Frequently, it is produced as a “by-product” of another process. Our world has seen an explosion in the amount of data available. We have witnessed numerous data explosions throughout history. Moreover, each time, the data increased by several orders of magnitude at a phenomenal pace. This occurred in conjunction with the invention of paper and the printing press. Furthermore, it is a cycle that has been repeated numerous times since the advent of electronics and modern digital media.<sup>2</sup> “The global data explosion is being fueled in part by technological advancements such as digital video and music, smartphones, and the internet’s growth.”<sup>3</sup>

---

<sup>1</sup> Software & Information Industry Association, White Paper on Data-Driven Innovation A Guide for Policymakers: Understanding and Enabling the Economic and Social Value of Data (2013), <https://history.siiia.net/Portals/0/pdf/Policy/Data%20Driven%20Innovation/data-driven-innovation.pdf> (last visited Oct 2, 2021); Abu Bakar Munir, Siti Hajar Mohd Yasin & Firdaus Muhammad-Sukki, *Big Data: Big Challenges to Privacy and Data Protection*, 9 WORLD ACADEMY OF SCIENCE, ENGINEERING AND TECHNOLOGY INTERNATIONAL JOURNAL OF COMPUTER AND INFORMATION ENGINEERING 355-363 (2015).

<sup>2</sup> Michael Wu, Big Data analytics: Turning zettabytes of data into actionable information MyCustomer (2012), <https://www.mycustomer.com/marketing/data/big-data-analytics-turning-zettabytes-of-data-into-actionable-information> (last visited Oct 1, 2021).

<sup>3</sup> Meeting the Challenge of Big Data: Part One, (2012), <https://www.oracle.com/webfolder/s/assets/ebook/bigdata/index.html> (last visited Oct 1, 2021).

Data has evolved into a manufacturing raw material and a new source of enormous economic and social value. The advancements in data mining and analytics and the massive increase in computing power and data storage capacity have increased the scope of information available to businesses, governments, and individuals by orders of magnitude. The amount of data being stored and generated on a global scale is increasing at such a rapid rate that scientists have had to coin new terms, such as zettabyte and yottabyte, to describe the onslaught of data.<sup>4</sup>

Statista forecasts that 79 zettabytes of data will be created in 2021. That is more than double the amount of data produced just two years ago, and growth at this rate is expected to continue indefinitely.<sup>5</sup> According to IDC, the global datasphere will reach 163 zettabytes (a trillion gigabytes) by 2025. That is ten times the data generated in 2016 (16.1ZB).<sup>6</sup>

“Businesses collect trillions of bytes of data about their customers, suppliers, and operations, and millions of networked sensors are embedded in the physical world in devices like mobile phones and automobiles, sensing, creating, and communicating data. The proliferation of multimedia and the use of smartphones and social networking sites will continue to drive exponential growth. Big data—vast pools of data that can be captured, communicated, aggregated, stored, and analyzed—is now ingrained in virtually every sector and function of the global economy. As is increasingly the case with other critical factors of production such as physical assets and human capital, much of contemporary economic activity, innovation, and growth would be impossible without data.”<sup>7</sup>

---

<sup>4</sup> C. Kuner et al., *The Challenge of 'Big Data' for Data Protection*, 2 INTERNATIONAL DATA PRIVACY LAW 47-49 (2012); Abu Bakar Munir, Siti Hajar Mohd Yasin & Firdaus Muhammad-Sukki, *Big Data: Big Challenges to Privacy and Data Protection*, 9 WORLD ACADEMY OF SCIENCE, ENGINEERING AND TECHNOLOGY INTERNATIONAL JOURNAL OF COMPUTER AND INFORMATION ENGINEERING 355-363 (2015).

<sup>5</sup> Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2025(in zettabytes), Statista (2021), <https://www.statista.com/statistics/871513/worldwide-data-created/> (last visited Oct 1, 2021).

<sup>6</sup> David Reinsel, John Gantz & John Rydning, *Data Age 2025: The Evolution of Data to Life-Critical Don't Focus on Big Data; Focus on the Data That's Big*, An IDC White Paper Sponsored by Seagate (2017), <https://www.import.io/wp-content/uploads/2017/04/Seagate-WP-DataAge2025-March-2017.pdf> (last visited Oct 1, 2021).

<sup>7</sup> James Manyika et al., *Big Data: The Next Frontier For Innovation, Competition, And Productivity*, McKinsey Global Institute (2011).

## 2.2 WHAT IS BIG DATA

“Erik Larson may have coined the term Big Data (without capitalization) in the manner in which it is used today in an article for Harpers Magazine in 1989. In 1999, the term “Big Data” appeared in the Association for Computing Machinery’s publication Visually Exploring Gigabyte Datasets in Real-Time. In 2001, in his paper 3D Data Management: Controlling Data Volume, Velocity, and Variety. Doug Laney, an analyst at Gartner, defines three of the characteristics of Big Data that will eventually become widely accepted. ‘Wired’ popularised the concept of Big Data in 2007 with their article The End of Theory: How the Data Deluge Will Destroy the Scientific Model.”<sup>8</sup>

The term “big data” is a relative term that varies according to who is discussing it.<sup>9</sup> “As one of the most “hyped” terms in today’s market, there is currently no agreement on how to define big data. Frequently, the term is used interchangeably with closely related concepts such as business intelligence (BI) and data mining. True, all three terms refer to data analysis, and in many cases, advanced analytics. However, big data differs from the other two concepts in that it refers to data volumes, transaction volumes, and the number of data sources that are so large and complex that they necessitate the use of specialized methods and technologies to extract insight from the data (for instance, traditional data warehouse solutions may fall short when dealing with big data). This also serves as the foundation for the most frequently used definition of big data, namely the three V’s.: Volume, Velocity, and Variety.”<sup>10</sup>

There are various definitions available for Big Data. Some of the prominent ones are:

According to Gartner, “Big data is high-volume, high-velocity, and/or high-variety information assets that demand cost-effective, innovative forms of information processing that enable enhanced insight, decision making, and process automation.”<sup>11</sup>

---

<sup>8</sup> Bernard Marr, A brief history of big data everyone should read World Economic Forum (2015), <https://www.weforum.org/agenda/2015/02/a-brief-history-of-big-data-everyone-should-read/> (last visited Oct 1, 2021).

<sup>9</sup> Keith D. Foote, A Brief History of Big Data DATAVERSITY (2017), <https://www.dataversity.net/brief-history-big-data/> (last visited Oct 1, 2021).

<sup>10</sup> Xiaomeng Su, Introduction to Big Data, Institutt for informatikk og e-l ring ved NTNU (2018), <https://lagesoft.files.wordpress.com/2018/11/bd-introduction-to-big-data.pdf> (last visited Oct 1, 2021).

<sup>11</sup> Definition of Big Data - Gartner Information Technology Glossary, Gartner, <https://www.gartner.com/en/information-technology/glossary/big-data> (last visited Oct 1, 2021).

According to Oracle, “The definition of big data is data that contains greater variety, arriving in increasing volumes and with more velocity. This is also known as the three Vs. Put simply, big data is larger, more complex data sets, especially from new data sources. These data sets are so voluminous that traditional data processing software just can’t manage them.”<sup>12</sup>

Analyst firm Forrester gives a pragmatic definition of big data “Big Data is the frontier of a firm’s ability to store, process, and access (SPA) all the data it needs to operate effectively, make decisions, reduce risks, and serve customers.”<sup>13</sup>

According to IBM, “Big data is a term applied to data sets whose size or type is beyond the ability of traditional relational databases to capture, manage and process the data with low latency. Big data has one or more of the following characteristics: high volume, high velocity or high variety.”<sup>14</sup>

J. Steven Perry in IBM Developer Blog gives the following definition, “The term Big Data really means “harvesting meaning from data” that is coming in faster, from more sources, and in more varied formats than ever before. We should probably call it Big Meaning. Because Big Data is really about the value (meaning) in the data, rather than the data itself.”<sup>15</sup>

While noting that there was no universally accepted definition, the White House’s Executive Office of the President (EOP) provided a useful description in a report dated 1 May 2014<sup>16</sup>: “Most definitions reflect the growing technological ability to capture, aggregate, and process an ever-greater volume, velocity, and variety of data. In other words, “data is now available faster, has greater coverage and scope, and includes new

---

<sup>12</sup> What Is Big Data? | Oracle, Oracle.com, <https://www.oracle.com/big-data/what-is-big-data/> (last visited Oct 1, 2021).

<sup>13</sup> Mike Gualtieri, The Pragmatic Definition of Big Data Forrester (2012), [https://www.forrester.com/blogs/12-12-05-the\\_pragmatic\\_definition\\_of\\_big\\_data/](https://www.forrester.com/blogs/12-12-05-the_pragmatic_definition_of_big_data/) (last visited Oct 1, 2021).

<sup>14</sup> Big Data Analytics, Ibm.com, <https://www.ibm.com/in-en/analytics/hadoop/big-data-analytics> (last visited Oct 1, 2021).

<sup>15</sup> J. Steven Perry, What is big data? More than volume, velocity and variety... IBM Developer Blog (2017), <https://developer.ibm.com/blogs/what-is-big-data-more-than-volume-velocity-and-variety/> (last visited Oct 1, 2021).

<sup>16</sup> *Big Data: Seizing Opportunities, Preserving Value* (2014), [https://obamawhitehouse.archives.gov/sites/default/files/docs/big\\_data\\_privacy\\_report\\_may\\_1\\_2014.pdf](https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf) (last visited Oct 1, 2021).

types of observations and measurements that previously were not available.”<sup>17</sup> More precisely, big datasets are “large, diverse, complex, longitudinal, and/or distributed datasets generated from instruments, sensors, Internet transactions, email, video, click streams, and/or all other digital sources available today and in the future.”<sup>18</sup>

The term “Big Data” is a bit of a misnomer because it implies that preexisting data is somehow insignificant (which it is not) or that the only issue is its sheer size (size is one of them, but there are often more). In a nutshell, Big Data refers to data that cannot be processed or analyzed using conventional methods or tools.<sup>19</sup>

“Additionally, it is necessary to emphasize that defining an absolute threshold for what constitutes big data may not be beneficial. As technologies advance, today’s big data may not be tomorrow’s big data. By and large, it is a relative concept.”<sup>20</sup>

### 2.3 CHARACTERISTICS OF BIG DATA

Initially, big data was defined in terms of the following dimensions, which are frequently referred to as the 3V model: volume, velocity, and variety. The 3V’s definition was first introduced in 2001 by Doug Laney, a Gartner Inc. analyst.<sup>21</sup>

Volume refers to the fact that Big Data analysis typically begins with tens of terabytes of data.<sup>22</sup>

“Velocity is a measure of the rate at which data is generated and changes. For instance, the data associated with a particular hashtag on Twitter is frequently updated at a rapid

---

<sup>17</sup> *Id*; See, Liran Einav and Jonathan Levin, “The Data Revolution and Economic Analysis,” Working Paper, No. 19035, *National Bureau of Economic Research*, 2013; VIKTOR MAYER-SCHONBERGER AND KENNETH CUKIER, *BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK*, (Houghton Mifflin Harcourt, 2013).

<sup>18</sup> *Big Data: Seizing Opportunities, Preserving Value* (2014), [https://obamawhitehouse.archives.gov/sites/default/files/docs/big\\_data\\_privacy\\_report\\_may\\_1\\_2014.pdf](https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf) (last visited Oct 1, 2021); National Science Foundation, Solicitation 12-499: *Core Techniques and Technologies for Advancing Big Data Science & Engineering (BIGDATA)*, 2012.

<sup>19</sup> PAUL C. ZIKOPOULOS ET AL., *UNDERSTANDING BIG DATA: ANALYTICS FOR ENTERPRISE CLASS HADOOP AND STREAMING DATA* (2012).

<sup>20</sup> *Supra* note 10.

<sup>21</sup> Big Data: What it is and why it matters, Sas.com, [https://www.sas.com/en\\_us/insights/big-data/what-is-big-data.html](https://www.sas.com/en_us/insights/big-data/what-is-big-data.html) (last visited Oct 1, 2021).

<sup>22</sup> Ian Mitchell, *The White Book of Big Data* (2012), <https://www.fujitsu.com/se/imagesgig5/WhiteBookofBigData.pdf> (last visited Oct 1, 2021).

rate. Tweets pass by in a flash. In some cases, they move so quickly that the data they contain cannot be easily stored but still needs to be analyzed.”<sup>23</sup>

Variety refers to the fact that Big Data can originate from a variety of different sources and be stored in a variety of different formats and structures. For instance, social media platforms and sensor networks generate a constant stream of data. Along with text, this may include geographic data, images, videos, and audio.<sup>24</sup>

Two additional V’s have emerged in recent years: value and veracity.<sup>25</sup>

“Value is a more nuanced concept. It is frequently quantified in terms of the social or economic value that the data may generate. However, the entire concept is imprecise, as, without proper intention or application, highly valuable data may sit idle in the warehouse. This is frequently the case when the actors who generate the data are not necessarily capable of valorizing it.”<sup>26</sup>

In general, veracity is defined as a data set’s accuracy or truthfulness.<sup>27</sup>

If none of the elements is present, the phenomenon being studied is most emphatically not Big Data; if all of the elements are present, the phenomenon being studied is most emphatically Big Data.

## 2.4 SOURCES OF BIG DATA

There are numerous sources of big data, including both human and machine-generated data feeds. The term “big data” refers to a collection of various granular data types. The primary sources of massive amounts of data are the Internet of Things (IoT), self-quantified, multimedia, and social media data.<sup>28</sup> “Data collection from sources such as

---

<sup>23</sup> *Id.*

<sup>24</sup> *Id.*

<sup>25</sup> Big Data: What it is and why it matters. [https://www.sas.com/en\\_us/insights/big-data/what-is-big-data.html](https://www.sas.com/en_us/insights/big-data/what-is-big-data.html)

<sup>26</sup> Samuel Cristobal, Two more V’s in Big Data: Veracity and Value - Datascience.aero Datascience.aero (2020), <https://datascience.aero/big-data-veracity-value/> (last visited Oct 1, 2021).

<sup>27</sup> *Id.*

<sup>28</sup> I.A.T. Hashem et al., *The Role of Big Data in Smart City*, 36 INTERNATIONAL JOURNAL OF INFORMATION MANAGEMENT 748–758 (2016); Ibrar Yaqoob et al., *Big data: From Beginning To Future*, 36 INTERNATIONAL JOURNAL OF INFORMATION MANAGEMENT 1231-1247 (2016).

online activity, RFID, instrumentation, social media, clickstreams, and trading systems is characterized by a high volume of transactions, a high rate of data flow, and a greater variety of data formats.”<sup>29</sup>

Big data is a collection of various granular data types. The applications that generate the bulk of data are the Internet of Things (IoT), self-quantified, multimedia, and social media data.<sup>30</sup> Several examples are provided here:

- “Web data. Customer-level web behaviour data can be captured, such as page views, searches, reading reviews, and purchasing. They can improve performance in areas such as next best offer, churn modelling, segmentation of customers, and targeted advertising.”<sup>31</sup>
- Text data is one of the most prevalent and widely used types of big data. Email, news, Facebook feeds, and documents are just a few examples.<sup>32</sup>
- “Time and location data. GPS, mobile phones, and Wi-Fi connections all contribute to the growth of time and location data. At the individual level, many organizations recognize the value of knowing when and where their customers are. Equally critical is an aggregated view of time and location data. As more people make their time and location data more publicly available, a plethora of interesting applications begin to emerge. Time and location data is one of the most sensitive categories of big data in terms of privacy and should be handled with extreme caution.”<sup>33</sup>
- “Smart grid and sensor data. Nowadays, sensor data is collected at an extremely high frequency from automobiles, oil pipelines, and wind turbines. Sensor data contains a wealth of information about the operation of engines and machinery. It enables a more rapid diagnosis of problems and the development of mitigation procedures.”<sup>34</sup>
- Social network data. Within social networking sites such as Facebook, LinkedIn, and Instagram, link analysis can be used to deduce a user’s network. Social network analysis can shed light on the types of advertisements that might appeal to particular

---

<sup>29</sup> *Supra* note 3.

<sup>30</sup> Ibrahim Abaker Targio Hashem et al., *The role of big data in smart city*, 36 *International Journal of Information Management* 748-758 (2016).

<sup>31</sup> *Supra* note 10.

<sup>32</sup> *Id.*

<sup>33</sup> *Id.*

<sup>34</sup> *Id.*

users. This is accomplished by taking into account not only the customers' stated interests but also those of their circle of friends or colleagues.<sup>35</sup>

“With the majority of big data sources, the power is not solely in what that particular source of data can tell you. The value is in the information that it can provide when combined with other data. It is truly the combination that matters.”<sup>36</sup>

## 2.5 HOW BIG DATA DIFFERS FROM TRADITIONAL DATA

According to ISO/IEC 2382-1, data are “a reinterpretable representation of information in a formalized manner, suitable for communication, interpretation or processing.”<sup>37</sup> This definition encompasses a broad range of data types, including geographical information, statistics, weather data, and research data.

There are several significant ways in which big data differs from more traditional data sources. “Bill Franks suggested the following distinctions between big data and traditional data sources in his book *Taming the big data tidal wave*: To begin, big data can represent an entirely new type of data. Second, one could argue that, at times, the speed of a data feed has increased to the point where it qualifies as a new data source. Thirdly, an increasing amount of semi-structured and unstructured data is being collected.”<sup>38</sup> “Structured data is the type of data used by traditional database systems, in which records are divided into well-defined ‘fields’ (such as ‘name,’ ‘address,’ etc.) that can be easily searched, classified, and sorted according to certain criteria. Meanwhile, unstructured data, such as image data or Twitter updates, lacks a clearly defined format. Semi-structured data is a synthesis of the two preceding types. While certain aspects of the data may be defined (typically within the information itself, for example, location data appended to social media updates), it lacks the rigidity associated with structured data.”<sup>39</sup>

---

<sup>35</sup> *Id.*

<sup>36</sup> *Id.*

<sup>37</sup> ISO/IEC 2382-1:1993(en) Information technology, Iso.org, <https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:-1:en> (last visited Oct 1, 2021).

<sup>38</sup> See, BILL FRANKS, *TAMING THE BIG DATA TIDAL WAVE* (2012); Xiaomeng Su, Introduction to Big Data, Institutt for informatikk og e-l ring ved NTNU (2018), <https://lagesoft.files.wordpress.com/2018/11/bd-introduction-to-big-data.pdf> (last visited Oct 1, 2021).

<sup>39</sup> *Supra* note 22.



## 2.6 BIG DATA VALUE CREATION

The concept of monetization aims to generate quantifiable economic benefits from both raw data and extracted resources. This can be accomplished in one of two ways: directly through the sale or sharing of data (explicit monetization) or indirectly through the enhancement of own data-based products (implicit monetization).

It is increasingly important for organizations to create value and achieve their goals by adapting their operating model to deal with daily generated data. However, processing and analyzing such a large volume of heterogeneous records using conventional tools and methods is not possible, as massively parallel processing techniques are required. As a result, it was necessary to introduce novel techniques that were compatible with the new standards. These methods and tools are referred to as Big Data analytics. Big Data analytics is the process of examining raw data, frequently in large quantities, in order to extract information that is understandable to humans but difficult to observe directly. Big Data analytics proposes a collection of tools for interacting with data in a variety of states. These tools fall into three broad categories: storage, processing, and visualization.

The Data Value Chain is a mechanism that defines a set of repeatable processes for extracting the value of data from raw data to verifiable insights. DVC is composed of four distinct steps: Data generation; Data collection; Data analysis, Data exchange. A Big Data system is often complex. A Big Data system enables an organization to consider Big Data's characteristics and act on that data to realize tangible benefits. It includes functions for managing the various stages of the lifecycle of digital data, from creation to destruction. As a result, it is critical to take a phase-by-phase approach to extract value from a typical process. BDVC is the abbreviation for this decomposition. The BDVC is composed of seven steps: (i) Data generation; (ii) Data acquisition; (iii) Data pre-processing; (iv) Data storage; (v) Data analysis; (vi) Data visualization; (vii) Data exposition.<sup>40</sup>

---

<sup>40</sup> Abou Zakaria Faroukhi et al., *Big Data Monetization Throughout Big Data Value Chain: A Comprehensive Review*, 7 JOURNAL OF BIG DATA (2020).

## 2.7 WHY BIG DATA MATTERS

“Over the last three decades, data has become critical to every aspect of human life; it has transformed how we are educated and entertained, and it shapes our perceptions of people, business, and the wider world. It is the lifeblood of our digital existence, which is growing at a breakneck pace. While we as consumers will reap the benefits of digital existence, businesses worldwide will seize new and unique business opportunities enabled by this wealth of data and the insight it provides. The volume and criticality of real-time data are astounding - from power grids and water systems to hospitals, public transportation, and road networks. Whereas data was once solely responsible for successful business operations, it is now a critical component of the smooth operation of all aspects of daily life for consumers, governments, and businesses alike.”<sup>41</sup>

Big Data has the potential to be used in virtually every sector and for virtually any task. Generally, three types of Big Data applications exist. To begin, the application of Big Data to specific government tasks. Second, the private or semi-public sector’s use of Big Data to assist or facilitate them in accomplishing their specific tasks or goals. Thirdly, both governments and private sector companies use Big Data to improve their service to citizens or customers; this may include increasing the transparency of their operations, strengthening citizen control over data processing, and so on.<sup>42</sup>

“According to IDC, nearly 20% of the data in the global datasphere will be critical to our daily lives by 2025, and nearly 10% will be hypercritical.”<sup>43</sup> These increasingly diverse data sets complement one another, allowing businesses to fill gaps and uncover new insights. Filling these gaps improves operational decision-making and provides components for improving business processes.<sup>44</sup> In his article “The Age of Big Data,” Steve Lohr pointed out that technological advancements pave the way for a new way

---

<sup>41</sup> *Supra* note 6.

<sup>42</sup> International and Comparative Legal Study on Big Data, WRR Working Paper 20, ‘Big Data, Privacy and Security’, Netherlands Scientific Council for Government Policy (WRR), (2016), <https://english.wrr.nl/publications/working-papers/2016/04/28/international-and-comparative-legal-study-on-big-data> (last visited Oct 1, 2021).

<sup>43</sup> *Supra* note 6.

<sup>44</sup> Mark Beyer & Douglas Laney, *The Importance of 'Big Data': A Definition*, Gartner (2012), Available at <http://www.gartner.com/doc/2595417>.

of understanding the world and making decisions.<sup>45</sup> Gartner predicts that by 2016, 30 per cent of businesses will be using their information assets as currency, bartering, trading, or even selling them.<sup>46</sup> “A report by the World Economic Forum, Big Data, Big Impact, declared data as a new class of economic asset, like currency or gold.”<sup>47</sup>

“Big data enables businesses to gain a deeper understanding of their users, customers, operations, supply chain, and even their competitive and regulatory environments. When properly utilized, big data can significantly improve business intelligence and result in improved services and decisions. Big data analytics can assist businesses in reducing costs and gaining a competitive edge.”<sup>48</sup>

“The impact of data abundance is far-reaching beyond the realm of business. Decisions in business, economics, and other fields will increasingly be made on the basis of data and analysis rather than experience and intuition. Big Data’s predictive power is being explored - and shows promise - in fields such as public health, economic development, and economic forecasting.”<sup>49</sup>

## **2.8 HOW BIG DATA CREATES VALUE**

“Big data does not in and by itself possess any value. People often assume that storing data creates value when, in fact, that has never happened. Big data is valuable only when you can get some insight into the data, and that insight can be used to build your decision-making. The power of big data lies in the analysis performed and the actions taken as a result of the findings.”<sup>50</sup>

---

<sup>45</sup> Steve Lohr, *The Age of Big Data*, The New York Times, 2012, <https://www.nytimes.com/2012/02/12/sunday-review/big-datas-impact-in-the-world.html> (last visited Oct 1, 2021).

<sup>46</sup> *Supra* note 44.

<sup>47</sup> Steve Lohr, *The Age of Big Data*, The New York Times, 2012, <https://www.nytimes.com/2012/02/12/sunday-review/big-datas-impact-in-the-world.html> (last visited Oct 1, 2021); See, World Economic Forum, Big Data, Big Impact: New Possibilities for International Development (2012), [https://www3.weforum.org/docs/WEF\\_TC\\_MFS\\_BigDataBigImpact\\_Briefing\\_2012.pdf](https://www3.weforum.org/docs/WEF_TC_MFS_BigDataBigImpact_Briefing_2012.pdf) (last visited Oct 1, 2021).

<sup>48</sup> *Supra* note 3.

<sup>49</sup> *Supra* note 45.

<sup>50</sup> *Supra* note 10.

Organizations will integrate and analyze data from a variety of sources, including social media, video, and smart mobile devices. Value extraction from big data is a multistage process that begins with raw data and ends with useful information. For a long time, organizations have derived useful information by combining mathematical modelling and sifting through massive amounts of data. Once refined, big data complements existing models and can provide a wealth of new insight for business intelligence applications. While data comes from a variety of sources, new insights are gained through an integrated analysis of all available data.<sup>51</sup>

There are mainly four categories through which Big Data analysis could be designed and conducted: prescriptive, predictive, diagnostic, and descriptive. Through any of these, companies could find correlations, identify patterns and create actionable insights. The descriptive analysis provides insight into the past and identifies what has happened; Predictive analysis aims to analyze scenarios of what might happen. Predictive analytics aims to identify patterns in data to determine the possibility of a project; Prescriptive analysis identifies which decisions should be taken into account. This is the most valuable type of analysis, as it usually generates rules and recommendations for the next steps; Diagnostic analysis allows to identify the causes leading to the achievement of a performance by looking at the past.<sup>52</sup>

Big data can benefit every industry and every organization. Big Data use cases across various industries categorized according to each industry are.<sup>53</sup>

---

<sup>51</sup> *Supra* note 3.

<sup>52</sup> Mandeep Kaur Saggi & Sushma Jain, *A Survey Towards an Integration of Big Data Analytics to Big Insights for Value-Creation*, 54 INFORMATION PROCESSING & MANAGEMENT 758-790 (2018); THOMAS ERL, WAJID KHATTAK & PAUL BUHLER, *BIG DATA FUNDAMENTALS: CONCEPTS, DRIVERS & TECHNIQUES* (2016); THOMAS ERL, ZAIGHAM MAHMOOD & RICHARDO PUTTINI, *CLOUD COMPUTING: CONCEPTS, TECHNOLOGY & ARCHITECTURE*, PRENTICE HALL SERVICE TECHNOLOGY SERIES FROM THOMAS ERL. (2013); Jiannong Cao et al., *Programming Platforms for Big Data Analysis*, in HANDBOOK OF BIG DATA TECHNOLOGIES 65-99 (Albert Y. Zomaya & Sherif Sakr 1 ed. 2017); Amy Shi-Nash & David R. Hardoon, *Data Analytics and Predictive Analytics in the Era of Big Data*, in INTERNET OF THINGS AND DATA ANALYTICS HANDBOOK 329-345 (Hwaiyu Geng 1 ed. 2016); CAROL L STIMMEL, *BIG DATA ANALYTICS STRATEGIES FOR THE SMART GRID* (2014); Safanaz Heidari et al., *Big data clustering with varied density based on MapReduce*, 6 JOURNAL OF BIG DATA (2019); Addi Ait-Mlouk, Tarik Agouti & Fatima Gharnati, *Mining and Prioritization of Association Rules for Big Data: Multi-Criteria Decision Analysis Approach*, 4 JOURNAL OF BIG DATA (2017).

<sup>53</sup> Top Big Data Analytics Use Cases, (2020), <https://www.oracle.com/a/ocom/docs/top-22-use-cases-for-big-data.pdf> (last visited Oct 1, 2021); The IBM Big Data Platform, (2013), <https://tdwi.org/~media/692A428D271F4D648BF6732EF0120EC0.PDFDF&usg=AOvVaw1Z4hQ-jGAgNf4SQxBODnX8> (last visited Oct 1, 2021).

- Manufacturing- Predictive maintenance, Operational efficiency, Production optimization;
- Retail - Product development, Customer experience, Customer lifetime value, The in-store shopping experience, Pricing analytics, and optimization;
- Healthcare - Genomic research, Patient experience, and outcomes, Claims fraud, Healthcare billing analytics;
- Oil and gas - Predictive equipment maintenance, Oil exploration, and discovery, Oil production optimization;
- Telecommunications - Optimize network capacity, Telecom customer churn, New product offerings;
- Financial Services - Fraud and compliance, Drive innovation, Anti-money laundering, Financial regulatory and compliance analytics;
- Transportation - Logistics optimization, Traffic congestion;
- Digital media - Real-time ad targeting, Website analysis.

“Big Data enables organizations to leverage a combination of existing data, transient data, and externally available data sources to generate additional value through the increased business intelligence that results in more informed decision-making and treating data as a tradable and sellable asset. Organizations must maintain a long-term perspective on Big Data — integrating multiple data sources in order to unlock even more potential value — while also ensuring that their current technology does not obstruct accuracy, immediacy, and flexibility.”<sup>54</sup>

## **2.9 CHALLENGES POSED BY BIG DATA TO PRIVACY**

Big Data presents enormous economic growth opportunities in a wide variety of fields, including national security, medical research, engineering, and technology, to name a few. However, public and private concerns about Big Data privacy have grown. The widely recognized privacy concerns arise as a result of the blurring of the lines between

---

<sup>54</sup> *Supra* note 22.

government, business, and the individual, which may result in social problems such as racial profiling, discrimination, or restriction of freedom.<sup>55</sup>

Big Data can be used in ways that have a direct impact on individuals. There are techniques for creating profiles and forecasting the behaviour of individuals and groups of individuals based on the compilation and analysis of personal data from a variety of different sources. While the data may be aggregated and de-identified, the analysis's outcome may still have implications for individuals.<sup>56</sup>

There are significant privacy challenges in the domain of Big Data for a variety of reasons, including the availability of data via multiple channels, such as mobile devices with location-tracking capabilities. Additionally, infrastructure advancements such as the availability of high-speed data transfer networks and stable operating systems. Along with large storage capacities and high-efficiency data processors, cloud computing and computational frameworks such as Apache Hadoop all contribute to Big Data's privacy concerns. Another barrier to privacy in Big Data is the ability to extract and interpret data from sources such as internet logs, surveillance cameras, mobile phones, and credit and debit cards.<sup>57</sup>

Frequently, Big Data enables data subjects to be identified through the use of non-personal data. This erodes anonymity, casting doubt on the fundamental distinction between personal and non-personal data.<sup>58</sup> Additionally, there are concerns about automated decision-making about an individual's life via automated processes in Big Data, such as benefits eligibility, credit ratings, or job prospects.<sup>59</sup> The ability to combine and mine data will result in the accumulation of more and more detailed information about individual lives.<sup>60</sup>

---

<sup>55</sup> Omer Tene and Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 NW. J. TECH. & INTELL. PROP. 239 (2013).

<sup>56</sup> International Working Group on Data Protection in Telecommunications, Working Paper on Big Data and Privacy principles under pressure in the age of Big Data analytics, (2014).

<sup>57</sup> Abu Bakar Munir, Siti Hajar Mohd Yasin & Firdaus Muhammad-Sukki, *Big Data: Big Challenges to Privacy and Data Protection*, 9 WORLD ACADEMY OF SCIENCE, ENGINEERING AND TECHNOLOGY INTERNATIONAL JOURNAL OF COMPUTER AND INFORMATION ENGINEERING 355-363 (2015); Yassir Elrayah, *Big Data: Intellectual Property and Legal Issues*, 1 IMPACT: JOURNAL OF DIGITAL INFORMATION TECHNOLOGY (2016).

<sup>58</sup> Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA LAW REVIEW 1701 (2010).

<sup>59</sup> Tene and Polonetsky, *supra* note 55.

<sup>60</sup> Yassir Elrayah, *Big Data: Intellectual Property and Legal Issues*, 1 IMPACT: JOURNAL OF DIGITAL INFORMATION TECHNOLOGY (2016).

Some of the significant privacy concerns that arise as a result of the use of Big Data are: Use of data for new purposes; Data maximization; Lack of transparency; Compilation of data may uncover sensitive information; Risk of re-identification; Security implications - challenges in terms of information security; Incorrect data; Power imbalance; Data determinism and discrimination; The Chilling effect; Echo chambers.<sup>61</sup>

In the majority of countries, Big Data initiatives are governed by existing legislation on privacy and data protection.<sup>62</sup>

## 2.10 CONCLUSION

Big Data comes from a variety of sources and originates from all over.<sup>63</sup> “The variety of information sources available is expanding at a breakneck pace. Along with social media data, there is telemetry data generated by cars, GPS data generated by smartphones, and information collected on individuals and organizations by banks and governments — and much more data is being generated on a continual basis.”<sup>64</sup>

Big data is a widespread occurrence that is not confined to a few industries. In the United States, an average business in any sector is estimated to have at least ten terabytes (TB) of data, and many have more than one petabyte (PB).<sup>65</sup>

“The question is how all of these sources can be applied to benefit a business while also establishing trust in the organizations and institutions that collect, handle, integrate, analyze, and act on that data. Additionally, businesses must understand the implications

---

<sup>61</sup> International Working Group on Data Protection in Telecommunications, Working Paper on Big Data and Privacy principles under pressure in the age of Big Data analytics, (2014); Omer Tene and Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 Nw. J. Tech. & Intell. Prop. 239 (2013).

<sup>62</sup> *Supra* note 42.

<sup>63</sup> Abu Bakar Munir, Siti Hajar Mohd Yasin & Firdaus Muhammad-Sukki, *Big Data: Big Challenges to Privacy and Data Protection*, 9 WORLD ACADEMY OF SCIENCE, ENGINEERING AND TECHNOLOGY INTERNATIONAL JOURNAL OF COMPUTER AND INFORMATION ENGINEERING 355-363 (2015).

<sup>64</sup> *Supra* note 22.

<sup>65</sup> Leslie Johnston, How many Libraries of Congress does it take?” The Signal: Digital Preservation Library of Congress (2012), <https://blogs.loc.gov/thesignal/2012/03/how-many-libraries-of-congress-does-it-take/>. (last visited Oct 2, 2021).

of relying on specific data sources and what they would do if those data sources were to become unavailable for any reason.”<sup>66</sup>

“Big Data is not a new or isolated phenomenon but rather a continuation of a long history of data collection and use. As with previous significant advancements in data storage, data processing, and the Internet, Big Data is merely another step toward fundamentally altering how we conduct business and society. Simultaneously, it will lay the groundwork for numerous evolutions.”<sup>67</sup>

Big data poses both risks and opportunities for both businesses and individuals. Not only are organizations experimenting with new ways to analyze, exploit, and monetize the data contained within, they are also grappling with the cost and risk associated with storing that data. On the one hand, the majority of people now have instant access to massive amounts of information, which has a variety of benefits, including spurring innovation, communication, and freedom of expression. On the other hand, these new data pools contain information about individuals, and the use of big data tools to combine and analyze this data could result in massive privacy violations.<sup>68</sup>

There are legal concerns regarding privacy and intellectual property protection surrounding big data. For example, there is no legal framework in place to safeguard personal and business data in Big Data. Additionally, a legal framework that clearly defines and explains the rights and responsibilities associated with Big Data will not only mitigate risk but will also become a necessary component of successful Big Data projects. Organizations should adopt a data protection policy for Big Data in all of its manifestations, including copyright, patent, and trademark. Nonetheless, data protection must strike a balance between threats and opportunities.<sup>69</sup> Big data carries a plethora of benefits and promises. Nonetheless, the threats to privacy and data protection are far too grave to ignore.<sup>70</sup>

---

<sup>66</sup> *Supra* note 22.

<sup>67</sup> *Supra* note 8.

<sup>68</sup> Richard Cumbley & Peter Church, *Is “Big Data” Creepy?*, 29 *COMPUTER LAW & SECURITY REVIEW* 601-609 (2013); Abu Bakar Munir, Siti Hajar Mohd Yasin & Firdaus Muhammad-Sukki, *Big Data: Big Challenges to Privacy and Data Protection*, 9 *WORLD ACADEMY OF SCIENCE, ENGINEERING AND TECHNOLOGY INTERNATIONAL JOURNAL OF COMPUTER AND INFORMATION ENGINEERING* 355-363 (2015).

<sup>69</sup> Elrayah, *supra* note 60.

<sup>70</sup> Munir and Yasin, *supra* note 63.



## **CHAPTER III:**

### **BIG DATA AND INTELLECTUAL PROPERTY RIGHTS**

#### **3.1 INTRODUCTION**

The demand for intellectual property is increasing at a rate never seen before. Intellectual property is a type of property that is created through the application of human intellect. Intellectual Property Rights (IPR) is a broad term that encompasses a variety of concepts, including patents, “trade secrets,” copyrights, trademarks, service marks, and designs. Each element of intellectual property is founded on knowledge. Intellectual property is a business's intangible asset. It instils confidence in business partners and financial institutions to invest in or collaborate with the organization in order to grow the business and maximize profits. Apart from safeguarding their creations, business owners can increase the value of their intellectual property in a variety of ways. They can franchise, license, or otherwise commercialize their intellectual property on a global scale. The more a property is explored globally, the more profit the owner earns. It is critical to recognize and protect such properties in the current era of global industrialization.

Intellectual property refers to a person's ability to create something new and present it. The owner, i.e., the producer, has a right to the property he creates with his own intellect. This type of property is invisible but can be felt through the senses. Intellectual property, regardless of species, is intangible incorporate property. In each case, it is a collection of rights pertaining to a specific material object created by the owner. Intellectual property is not a property right in the strict sense; instead, it is a monopoly right. The primary reason for protecting it is to foster creative endeavours and inventions. Intellectual Property Rights serve as the breeding ground for a system that attempts to balance the conflicting interests of private inventors or creators and the general public.

#### **3.2 INTELLECTUAL PROPERTY RIGHTS CONCERNING DATA**

Copyright, Sui Generis Database Rights, and Trade Secrets are the primary intellectual property rights associated with data. Trademarks may be used on data products (such as indices) but not on the raw data in general. Patents and other forms of intellectual property can be used to protect only software and business processes that manipulate and process data, not the data itself.<sup>71</sup>

### 3.2.1 COPYRIGHT

Copyrights safeguard the author's original works.<sup>72</sup> “Copyright is a legal term that refers to the authors' rights to their literary and artistic works. Copyright protects a wide variety of works, including books, music, paintings, sculpture, and films, as well as computer programs, databases, advertising, maps, and technical drawings. Copyright protection applies exclusively to expressions, not to concepts, processes, methods of operation, or mathematical expressions in general.”<sup>73</sup>

Databases are protected under copyright rules in the majority of nations. Databases are defined differently in different countries, as are the legal interpretations of copyright protection. The argument has centred on the intellectual capabilities required to create databases. Numerous databases fail to meet the bare minimum requirements for copyright protection under applicable legislation.<sup>74</sup>

“Article 10(2) of the TRIPS Agreement<sup>75</sup> and Article 5 of the WIPO Copyright Treaty<sup>76</sup> provide copyright protection for compilations of data or other materials that constitute an intellectual creation “by virtue of their selection and arrangement”.”<sup>77</sup> Article 2(5) of the Berne Convention provided copyright on authors' literary and artistic collections,

---

<sup>71</sup> Richard Kemp, *Legal aspects of Managing Big Data*, 30 COMPUTER LAW & SECURITY REVIEW 482-491 (2014).

<sup>72</sup> A. K KOUL & V. K AHUJA, THE LAW OF INTELLECTUAL PROPERTY RIGHTS (2001).

<sup>73</sup> Copyright, Wipo.int, <https://www.wipo.int/copyright/en/> (last visited Sep 30, 2021).

<sup>74</sup> V.K. Gupta, *Copyright Issues Relating to Database Use*, 17 DESLDOC BULLETIN OF INFORMATION TECHNOLOGY 11-16 (1997).

<sup>75</sup> Agreement on Trade-Related Aspects of Intellectual Property Rights, (1995) [https://www.wto.org/english/docs\\_e/legal\\_e/31bis\\_trips\\_01\\_e.htm](https://www.wto.org/english/docs_e/legal_e/31bis_trips_01_e.htm) (last visited Sep 30, 2021).

<sup>76</sup> WIPO Copyright Treaty (WCT) (1996), <https://wipolex.wipo.int/en/text/295157> (last visited Sep 30, 2021). [hereinafter WCT]

<sup>77</sup> Compare TRIPS art. 10(2) with WCT art. 5. Basic Proposal for the Substantive Provisions of the Treaty on Certain Questions Concerning the Protection of Literary and Artistic Works to be considered by the Diplomatic Conference CRNR/DC/4, In Diplomatic Conference on Certain Copyright and Neighboring Rights Questions (1996), [https://www.wipo.int/edocs/mdocs/diplconf/en/crn\\_r\\_dc/crn\\_r\\_dc\\_4.pdf](https://www.wipo.int/edocs/mdocs/diplconf/en/crn_r_dc/crn_r_dc_4.pdf) (last visited Sep 30, 2021). (According to the Explanatory Notes, no differences were seen between the words “collection” and “compilation”).

“which constitutes an intellectual creation by reason of the selection and arrangement of their contents.”<sup>78</sup>

Copyright laws protect databases as collections or compilations of literary and creative works. The fundamental criterion is that a database is the product of its creator's intellectual work and exhibits a sufficient degree of originality.<sup>79</sup>

WCT protects compilations of data or other material in any form that constitutes intellectual creations due to the selection or arrangement of their contents. Without such a creation, a database is not covered by the Treaty.<sup>80</sup>

Copyright protection is also available for data compilations, which is critical in the context of Big Data. Under the US Copyright Law, the compilation is defined as “a work formed by the collection and assembling of preexisting materials or of data that are selected, coordinated, or arranged in such a way that the resulting work as a whole constitutes an original work of authorship. The term compilation includes collective works.”<sup>81</sup> A compilation of purely factual information is not protected by copyright. Rather than that, a compilation may be copyrighted only if it contains a creative or original act, such as the selection and arrangement of materials. The protection is limited to the compilation's creative or original aspects.<sup>82</sup>

Prior to 1991, the United States Supreme Court held that the “sweat of the brow” doctrine applied to factual compilations, or “industrial collections”.<sup>83</sup> Two years after the Berne Convention was ratified, US courts reversed their earlier decisions, rejecting the “sweat of the brow” doctrine and establishing rules to protect factual compilations from copyright infringement. The US courts began to recognize and value the author's creativity in his works rather than simply his sweat. Labour contributions made during

---

<sup>78</sup> Berne Convention for the Protection of Literary and Artistic Works Paris Act of July 24, 1971, as amended on September 28, 1979, <https://wipolex.wipo.int/en/text/283693> (last visited Sep 30, 2021), art. 2(5).

<sup>79</sup> Gupta, *supra* note 74.

<sup>80</sup> WCT, art 5.

<sup>81</sup> 17 U.S. Code § 101- Definitions.

<sup>82</sup> 17 U.S. Code § 103 - Subject Matter of Copyright: Compilations and Derivative Works

<sup>83</sup> *Hutchinson v. Fronteer*, 770 F.2d 128 (1985) (8th. Cir. 1989) (Concerning copyrightable telephone directories); *Applied Innovations, Inc. v. Regents of Univ. of Minn.*, 876 F.2d 626, 634-35 (8th. Cir. 1989) (Concerning copyrightable data of a psychological test only as compilations); *Dow Jones & Company, Inc., v. Board of Trade of the City of Chicago* 546 F. Supp. 113 (1982) (Concerning copyrightable lists of component stocks) and in *List Pub. Co. v. Keller*, 30 F. 772 (1887) (Concerning copyrightable society directories).

the collection and compilation of facts or data were no longer protected by copyright in factual compilations. The Supreme Court, in the landmark case *Feist Publications, Inc. v. Rural Telephone Service Co., Inc.* (1991)<sup>84</sup>, required proof of an author's creative expression in the selection and arrangement of a factual compilation. The case concerned raw data, specifically the names and addresses of subscribers as listed in telephone directories. The Supreme Court of the United States established two propositions: (a) facts are not copyrightable, and (b) compilations of facts are.<sup>85</sup> The Supreme Court held that the compilation must contain some element of originality, even if it is minimal. A chronological, sequential, or alphabetical listing of data is unlikely to suffice; however, another grouping that reflects the exercise of subjective judgment is likely to suffice.<sup>86</sup>

“When Big Data is initially collected, it is most often unstructured and raw. As a result, the majority of spending on Big Data is on software and personnel to organize the data. Copyright may apply to the compilation of data into a format that reflects a corporation's judgment and efforts. Notably, the individual pieces of data that comprise the compilation are not protected under copyright law—a significant shortcoming of the law. As the Supreme Court of the United States noted in *Feist Publications*, “raw facts may be copied at will.”<sup>87</sup>

Directive on Databases by the European Union<sup>88</sup> provides copyright protection for databases within the EU. The Directive applies to data compilations in any form, including hard copy compilations and electronic databases.<sup>89</sup> The Directive's copyright section, Chapter II, applies only to a database's structure or schema, without prejudice to any existing copyright protection for the database's contents.<sup>90</sup> According to the

---

<sup>84</sup> *Feist Publications, Inc. v. Rural Telephone Service Co., Inc.*, 499 U.S. 340, 111 S. Ct. 1282 (1991).

<sup>85</sup> *Id.* at 345.

<sup>86</sup> Paven Malhotra, *How Big Data and IP Intersect Big Data is big business—but who owns it?*, Intellectual Property an ALM Supplement to Corporate Counsel, 2016, [https://www.keker.com/Templates/media/files/Articles/How%20Big%20Data%20and%20IP%20Intersect\\_Malhotra.pdf](https://www.keker.com/Templates/media/files/Articles/How%20Big%20Data%20and%20IP%20Intersect_Malhotra.pdf) (last visited Sep 30, 2021).

<sup>87</sup> *Id.*

<sup>88</sup> DIRECTIVE 96/9/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 March 1996 on the legal protection of databases, <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996L0009:EN:HTML> (last visited Sep 30, 2021). [hereinafter Database Directive]

<sup>89</sup> *Id.* art. 1(1), recital (14).

<sup>90</sup> *Id.* art. 3(2).

Directive's standard, the database must “constitute the author's intellectual creation” through “the selection or arrangement of [its] contents.”<sup>91</sup>

Traditional literary copyright exists in the context of data in the form of documentation, such as publications relating to research and stock market analysis and technical and user documentation pertaining to computer software and information architecture. Since 1985 and 1993, respectively, in the United Kingdom, computer programs and preparatory design material for a computer program have been protected as literary works. Moral rights are applicable to the copyright of literary works but not to software.<sup>92</sup>

Big data controllers frequently need to differentiate and correlate the data they collect. While the volume of data is enormous and constantly changing, it undoubtedly reflects the value preferences of big data controllers. As a result, the big data information obtained by data users from various big data controllers is frequently dissimilar and even diametrically opposed in arrangement, which naturally reflects their own information selection and arrangement. Conform to the compilation work's original requirements. As can be seen, protecting big data's copyright is a viable option.<sup>93</sup>

In the 1990s, data in typical databases were generally “structured,” and this structure may have qualified the database for (thin) copyright protection at the organizational layer. Additionally, older databases contained fewer datasets (“small data”) than modern databases. Indeed, Big Data is frequently defined in opposition to the SQL database concept, as reflected in the TRIPS Agreement and the EU database directive. It is highly improbable that Big Data software will “select or arrange” data in a way that triggers copyright protection. Some argue that copyright can be used to protect tables or other outputs such as TDM system analysis results.<sup>94</sup> Whether computer-

---

<sup>91</sup> *Id.* art. 3(1).

<sup>92</sup> Kemp, *supra* note 71.

<sup>93</sup> Meng Lu, *Intellectual Property Protection of Big Data*, 1693 JOURNAL OF PHYSICS: CONFERENCE SERIES 012012 (2020).

<sup>94</sup> Daniel Gervais, *Exploring the Interfaces Between Big Data and Intellectual Property Law*, 10 JOURNAL OF INTELLECTUAL PROPERTY, INFORMATION TECHNOLOGY AND E-COMMERCE LAW (2019).

generated works qualify as copyright works are either still unresolved or have been resolved in favour of the requirement of human authorship.<sup>95</sup>

While Big Data is protected by copyright, copyright protects the idea of expression rather than the idea itself<sup>96</sup>. This is counterproductive to protecting big data because it leaves the door open to competition. The majority of business and analytical solutions are simply expressions of mathematical models used to solve specific problems or identify patterns in collected data, which are themselves simply expressions of mathematical concepts<sup>97</sup>.

### 3.2.2 SUI GENERIS PROTECTION

“In Europe, database creators concluded that copyright protection was insufficient because it protected only creative data (photographic works, musical compositions, literary works, and so on) and copying, viewing, obtaining, and using the information in their databases, but not the database's factual contents (statistics, raw scientific data, and the like). They urged their national governments to protect and secure their investment in database industries by granting them a new right in factual and data contents - so-called sui generis rights - in addition to the existing copyright protection for creative selection and arrangement of information. Sui generis protection is not an authentic intellectual property right. Rather, it is a unique economic criterion used to protect the compiler's substantial investments in the databases.”<sup>98</sup>

---

<sup>95</sup> The US Copyright Office, for example takes that view, See, U.S. COPYRIGHT OFFICE, COMPENDIUM OF U.S. COPYRIGHT OFFICE PRACTICES § 101 (3d ed. 2021), at 3-4. See, Amir Khoury, *Intellectual Property Rights for Hubots: On the Legal Implications of Human-like Robots as Innovators and Creators*, 35 CARDOZO ARTS & ENT. LJ 635-665 (2016). For an older but potentially still relevant article on the same topic, see Daniel Gervais, *The Protection Under International Copyright Law of Works Created with or by Computers*, 5 IIC INT’L REV. IND’L PROP. AND COPYRIGHT LAW, 629, 644-45 (1991). For a critique, see Shlomit Yanisky-Ravid & Luis Antonio Luis Antonio Velez- Hernandez, *Copyrightability of Artworks Produced by Creative Robots and Originality: The Formality-Objective Model*, 19 MINNESOTA JOURNAL OF LAW, SCIENCE & TECHNOLOGY (2018). A recent proposal suggests applying the work-made-for-hire doctrine for AI works so that the human operating the AI system would be the author under US law. See Shlomit Yanisky-Ravid & Samuel Moorhead, *Generating Rembrandt: Artificial Intelligence, Accountability and Copyright - The Human-Like Workers Are Already Here - A New Model*, 2017 MICHIGAN STATE LAW REVIEW 659 (2017).

<sup>96</sup> See, Frequently Asked Questions: Copyright, wipo.int, [https://www.wipo.int/copyright/en/faq\\_copyright.html](https://www.wipo.int/copyright/en/faq_copyright.html) (last visited Sep 30, 2021).

<sup>97</sup> See, Stephen Baker, *Big Data and Math* Thenumerati.net (2012), <http://thenumerati.net/?postID=845&big-data-and-math> (last visited Sep 30, 2021).

<sup>98</sup> Chana Rungrojtanakul, *Legal Protection of Sui Generis Databases*, 2005, <https://digitalcommons.law.ggu.edu/cgi/viewcontent.cgi?article=1015&context=theses> (last visited Sep 30, 2021).

“Sui generis legislation was first introduced in the United States in 1996, but it has failed to pass so far.”<sup>99</sup>

Sui generis database rights were established in 1996 by the EU database directive<sup>100</sup>. The sui generis right is defined in Article 7 of the Database Directive. Sui generis database rights prohibit using or extracting data from a database without the creator's permission. They safeguard any database that has been created with a significant investment of time, money, and effort. Database creators may prohibit the extraction and/or re-use of the entirety or a substantial portion of their databases where it can be demonstrated that a significant investment has been made qualitatively and/or quantitatively in obtaining, verifying, or presenting the database's contents.<sup>101</sup> Substantial changes cause the database to be viewed as a significant new investment. It qualifies the updated database for its own protection period.<sup>102</sup>

The 1997 Copyright and Rights in Databases Regulations incorporated the Directive into UK law.

The new right does not clearly distinguish between the database itself and its contents as database copyright does. As a result, the database's underlying data may be protected. *British Horseracing Board Limited v William Hill Organization* (2001), the first UK decision on the sui generis right, confirmed this protection for underlying information. It is an investment in terms of financial resources and/or time, effort, and energy that should be protected, and the right's purpose should be to specifically protect such investment. Not merely parasitical competition, but also damage to this investment is being protected. This was a significant factor in *Laddie J's* and the Court of Appeal's interpretation of the Directive in *British Horseracing Board Ltd v William Hill Organisation* (2001).<sup>103</sup>

---

<sup>99</sup> H.R.3531 - Database Investment and Intellectual Property Antipiracy Act of 1996 104th Congress (1995-1996), <https://www.congress.gov/bill/104th-congress/house-bill/3531/text> (last visited Sep 30, 2021).

<sup>100</sup> Database Directive.

<sup>101</sup> Case C-46/02 *Fixtures Marketing Ltd v. Oy Veikkaus Ab* [2004] ECR I-10396 (ECJ); Case C-203/02 *British Horseracing Board v. William Hill Organization* [2004] ECR I-10415 (ECJ); Case C-338/02 *Fixtures Marketing Ltd v. Svenska Spel AB, Fixtures Marketing v. Svenska Spel* [2004] ECR I-10497 (ECJ); Case C-444/02 *Fixtures Marketing Ltd v. Organismos prognostikon agonon podosfairou AE (OPAP)* [2004] ECR I-10549

<sup>102</sup> Catherine Colston, *Sui Generis Database Right: Ripe for Review?*, 3 JOURNAL OF INFORMATION LAW & TECHNOLOGY (2001).

<sup>103</sup> *Id.*

“The database sui generis right is referred to as one of the most unbalanced and potentially anti-competitive intellectual property rights ever created.”<sup>104</sup> “The European Union's Database Directive has the potential to create an indefinite duration of protection. Article 10(3) of the EU Directive provides that it may be extended indefinitely if there is evidence of “any significant change, evaluated qualitatively or quantitatively, to the contents of a database, including any significant change resulting from the accumulation of successive additions, deletions, or alterations,”<sup>105</sup> which would result in the database being considered a substantially new investment. Such recurrent durations of protection would result in a lengthy and nearly infinite duration of protection, effectively creating a monopoly in the European database industries. Applying this to Big Data, data is being created every second in vast quantity. Such addition of data would mean that there has been a new investment made to the data compilation. This would, in turn, give perpetual protection to the Big Data compilation or collection.”<sup>106</sup>

The Directive refers to the database creator's investment in “obtaining, verifying, or presenting the contents” of a database and then grants the database maker the right “to prevent the extraction and/or re-utilization of the entire or a substantial portion” of that database.<sup>107</sup> Additionally, the Directive's recitals state that a database is “a collection of independent works, data, or other materials that are organized systematically or methodically and can be accessed individually.”<sup>108</sup> Professor Hugenholtz asserts that this precludes protection of raw machine-generated data – whether through copyright or sui generis rights.<sup>109</sup>

The use of NoSQL technologies may void the Big Data corpora's sui generis right. Additionally, it appears reasonable to assert that machine-generated outputs (such as

---

<sup>104</sup> Jerome H. Reichman & Pamela Samuelson, *Intellectual Property Rights in Data?*, 50 VANDERBILT LAW REVIEW 52-166 (1997), at 81; ESTELLE DERCLAYE, THE LEGAL PROTECTION OF DATABASES - A COMPARATIVE ANALYSIS (2008); ROBIN ELIZABETH HERR, IS THE SUI GENERIS RIGHT A FAILED EXPERIMENT (2008), at 122.

<sup>105</sup> Article 10(3) and recital 54. “... the burden of proof that the criteria exist for concluding that a substantial modification of the contents of a database is to be regarded as a substantial new investment lies with the of the database resulting from such investment.”

<sup>106</sup> Rungrojtanakul, *supra* note 98.

<sup>107</sup> Database Directive, art 7(1).

<sup>108</sup> *Id.* recital 7.

<sup>109</sup> P. Bernt Hugenholtz, *Data Property: Unwelcome Guest in the House of IP*, 3 *Kritika. Essays on Intellectual Property*. See also, Estelle Derclaye, *The Database Directive*, in EU COPYRIGHT LAW - A COMMENTARY 298–354 (Irina A. Stamatoudi & Paul Torremans 2014) at 302-303.



new data corpora) resulting from Big Data analyses are not “obtained” or “collected”; rather, they are generated by the machine. This would appear to imply that the sui generis right no longer protects them.<sup>110</sup>

The economic rationale for the Database Directive is to encourage and reward investment in database production, not in data generation.<sup>111</sup> This raises the question of whether the concept of investment is sufficient to justify the special treatment of Big Data corporations. However, according to Matthias Leistner, a broad conclusion that all sensor- or machine-generated data will typically be excluded from the sui generis right is not justified.<sup>112</sup>

“Perhaps an indirect confirmation that “Big Data” corpora are not protected by copyright or the sui generis database right can be found in a Commission staff document accompanying a 2017 Commission Communication in which the idea of establishing a data producer's right was floated.”<sup>113</sup> “The Staff document noted that the Database Directive did not create a new right in data. According to the European Court of Justice, neither the Directive's copyright protection nor the sui generis right is designed to protect the content of databases. The EC has also stated that the investment in creating data should not be considered when deciding whether a database can be protected under sui generis right.”<sup>114</sup>

### 3.2.3 TRADE SECRETS

“While copyright provides some protection for the individual pieces of data that make up a compilation, trade secret law provides more robust protection. Due to the fact that

---

<sup>110</sup> Gervais, *supra* note 94.

<sup>111</sup> See generally, *Database rights: the basics*, Pinsent Masons (2019), <https://www.pinsentmasons.com/out-law/guides/database-rights-the-basics> (last visited Sep 30, 2021).

<sup>112</sup> Matthias Leistner, *Big Data and the EU Database Directive 96/9/EC: Current Law and Potential for Reform*, SSRN Electronic Journal (2018).

<sup>113</sup> European Commission, Commission Staff Working Document on the free flow of data and emerging issues of the European data economy Accompanying the document Communication Building a European data economy {COM(2017) 9 final} (2017),

[https://ec.europa.eu/newsroom/dae/document.cfm?doc\\_id=41247](https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41247) (last visited Sep 30, 2021); See also, European Commission, Building A European Data Economy {SWD(2017) 2 final} (2017), <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0009&from=EN> (last visited Sep 30, 2021)..

<sup>114</sup> *Id.*

trade secret laws protect not only the compilation of data but also the underlying data, they provide businesses with an effective tool.”<sup>115</sup>

Trade secrets are confidential information that is protected by intellectual property rights and may be sold or licensed.<sup>116</sup> “Businesses across the economy routinely use trade secrets to safeguard their know-how and other commercially valuable information, thereby promoting competitiveness and innovation.”<sup>117</sup>

Big data satisfies the trade secret criteria for secrecy, value, and confidentiality. Firstly, big data satisfies the need for secrecy since its very nature is the gathering of information. The user agrees to provide his or her personal information to the big data controller, which must be based on a confidentiality agreement signed by both parties, which places the big data controller under a duty of confidentiality, which means that without a proper basis, the user information cannot be leaked. Naturally, big data controllers maintain the gathered information private in the event that rivals grab the market edge. Second, the business use of big data is self-evident. Massive big data is a country's and enterprise's secret weapon in the wave of the global economy. The intentional creation and analysis of this data create a valuable information resource that aids governments and businesses in making scientific decisions. Not only that, but big data controllers may also benefit from big data, which has significant economic worth. Finally, in terms of confidentiality, big data controllers often enhance the security of big data management via system updates to ward off hackers and avoid data breaches. To summarise, trade secrets may be used to safeguard large data.<sup>118</sup>

“The TRIPS Agreement requires that unpublished information be protected. According to Article 39.2, protection must be extended to information that is secret, has commercial value as a result of its secrecy, and has been subjected to reasonable safeguards to maintain its secrecy. The Agreement does not require that undisclosed information be treated as property, but it does require that a person lawfully in control of such information have the ability to prevent it from being disclosed to, acquired by,

---

<sup>115</sup> *Supra* note 86.

<sup>116</sup> Trade Secrets, wipo.int, <https://www.wipo.int/tradesecrets/en/> (last visited Sep 30, 2021).

<sup>117</sup> John Hull, *Protecting trade secrets: how organizations can meet the challenge of taking “reasonable steps”*, WIPO Magazine, 2019, [https://www.wipo.int/wipo\\_magazine/en/2019/05/article\\_0006.html](https://www.wipo.int/wipo_magazine/en/2019/05/article_0006.html) (last visited Sep 30, 2021).

<sup>118</sup> Lu, *supra* note 93.

or used by others in a manner inconsistent with honest commercial practices without his or her consent.”<sup>119</sup>

The Trade Secrets Directive (2016/943) has harmonized trade secret protection in the European Union to some extent. The European Union's Trade Secrets Directive (2016/943) protection extends to databases and their underlying data. The database's substantial and insubstantial portions are both protected. While the Trade Secrets Directive and the Database Directive overlap, the two are complementary.<sup>120</sup>

Trade secrets are governed in the United States by both state law (statutory (UTSA) and common law) and federal law. The Defend Trade Secrets Act of the United States protects data compilations. Databases are widely recognized as potential trade secrets, and this protection may also extend to the underlying methodologies used to collect, select, and refine the database. Obtaining a trade secret through reverse engineering, for example, is not prohibited by the law.<sup>121</sup>

“India, a signatory to the TRIPS Agreement, and Article 39 of the TRIPS Agreement protects natural and legal persons from disclosing information that qualifies as a trade secret. In India, the judiciary has decided to protect trade secrets under the Copyright Act, 1957, on the basis of equity and through a common-law action for breach of confidence, which equates to contractual breach due to the absence of a trade secret law. The court noted in *Zee Telefilms Ltd. & Anr. v. Sundial Communications Pvt. Ltd.*<sup>122</sup> that the law of breach of confidence is a broader right than proprietary copyright. In a breach of confidence case, the court considers the matter in terms of fairness. The unauthorized use of confidential information serves as a springboard for the infringer.”<sup>123</sup>

---

<sup>119</sup> WTO | Intellectual Property - Overview of TRIPS Agreement, wto.org, [https://www.wto.org/english/tratop\\_e/trips\\_e/intel2\\_e.htm](https://www.wto.org/english/tratop_e/trips_e/intel2_e.htm) (last visited Sep 30, 2021).

<sup>120</sup> Richard M. Assmus, Mark Prinsley & Lana Khoury, *IP Rights for Data: Mortaring Over the Cracks*, (2019), <https://www.mayerbrown.com/-/media/files/perspectives-events/events/2019/07/event190723chiwebinarttiprightsslides.pdf> (last visited Sep 30, 2021).

<sup>121</sup> *Id.*

<sup>122</sup> *Zee Telefilms Ltd. v. Sundial. Communications Pvt. Ltd.*, 2003 (27) PTC 457 (Bom).

<sup>123</sup> Trade Secrets Protection and Incentives to Innovate: Scrutinizing Section 91 of The Personal Data Protection Bill, 2019, SpicyIP (2020), <https://spicyip.com/2020/07/trade-secrets-protection-and-incentives-to-innovate-scrutinizing-section-91-of-the-personal-data-protection-bill-2019.html> (last visited Sep 30, 2021).

“Trade secrets come the closest to being the optimal method for protecting numerous types of data. It is permissible for a business to possess the same data as another business as long as the business collected or created the data independently and did not obtain it from the other business. According to some, trade secrets are a sham because not all data is kept secret, even when organizations do not want others to use it.”<sup>124</sup> Firstly, for databases that are intended to be marketed or shared, the requirement for secrecy is difficult to meet. The creator of the database could attempt to maintain secrecy by relying on contracts that forbid each customer from disclosing the information. It can be effective when the customer base is small and no information sharing is required. However, a system with a complex web of interested parties quickly becomes unsuitable for a contracts-based solution due to the high transaction costs associated with monitoring and controlling customer data exchange.<sup>125</sup>

Secondly, there is no clear and unified standard for classifying big data as a trade secret. To be more precise, to what extent must the confidentiality safeguards implemented by big data controllers be considered “reasonable”? How can the secrecy of big data be determined? As users leave traces of online shopping, browsing web pages, and so on, the collection of data information becomes more convenient and diverse, resulting in disagreements over how to define big data secrecy. Regrettably, current legislation does not provide a definitive answer to this question.<sup>126</sup> “Trade secrets do not confer on their holders any specific exclusivity rights. The point is not that the data is secret; rather, the data's “owner” wishes to restrict its use.”<sup>127</sup>

### 3.3 CONCLUSION

---

<sup>124</sup> Claudia Jamin, *Managing Big Data in the Digital Age: An Industry Perspective*, Intellectual Property and Digital Trade in the Age of Artificial Intelligence and Big Data 150 (2018), [https://static-curis.ku.dk/portal/files/203882663/ceipi\\_ictsd\\_issue\\_5\\_final\\_0.pdf](https://static-curis.ku.dk/portal/files/203882663/ceipi_ictsd_issue_5_final_0.pdf) (last visited Sep 30, 2021).

<sup>125</sup> Julie E. Cohen & William M. Martin, *Intellectual Property Rights in Data*, in INFORMATION SYSTEMS AND THE ENVIRONMENT 45-55 (Deanna J. Richards, Braden R. Allenby & W. Dale Compton 2001).

<sup>126</sup> Lu, *supra* note 93.

<sup>127</sup> Robert D. Atkinson, *IP Protection in the Data Economy: Getting the Balance Right on 13 Critical Issues* (2019), [https://www2.itif.org/2019-ip-protection-data-economy.pdf?\\_ga=2.177242277.1647718639.1632912651-1493660189.1632912651](https://www2.itif.org/2019-ip-protection-data-economy.pdf?_ga=2.177242277.1647718639.1632912651-1493660189.1632912651) (last visited Sep 30, 2021).

IP rights in relation to data are ambiguous, and the law in this area will continue to evolve in the coming years. The relationship between big data and intellectual property is about adjusting intellectual property rights to allow for and define appropriate parameters for the generation, processing, and use of big data. The vast majority of experts agree that current legislation in the majority of jurisdictions is woefully inadequate to address this complex issue. Courts and legislators will spend years debating the constraints on and protection of Big data. This includes an examination of how Big Data may infringe on intellectual property rights, but there is also a question of rights in Big data.

Due to the nature of the non-relational (NoSQL) databases that characterize Big Data, they are unlikely to be protected by copyright or the EU's sui generis database rights. Protecting data as trade secrets appears to be a viable option, but there is currently no clear and unified definition of what constitutes a trade secret. Maintaining data secrecy also jeopardizes the ability to protect data as a trade secret. Data cannot be patented because it is neither a physical invention nor a technical solution to a problem.

When it comes to data protection, we must distinguish between unprocessed data derived from individuals and processed data. The former is intimately linked to individuals and bears obvious identity characteristics, and as such, should be protected by privacy, whereas the latter is a product of big data technologies, requiring not only labour but also an economic investment.

Computer software performs the vast majority of the “work,” resulting in a significant gap between human creators and their digital tools. The logical conclusion is that authorship in big data should be re-examined. Thus, data protection and intellectual property laws combine to create a complicated ownership regime for data.

# CHAPTER IV:

## OWNERSHIP OF DATA

### 4.1 INTRODUCTION

According to the European Commission, “data has become an essential resource for economic growth, job creation, and societal progress.”<sup>128</sup> “Data's commercial value and economic importance have inevitably led to calls for an ownership right in data. The first ideas on the subject of data ownership were first raised decades ago.”<sup>129</sup>

In a strictly legal sense, raw data are not subject to property law.<sup>130</sup> Data is, without a doubt, an asset, if not the asset of the twenty-first century, in the big data era.<sup>131</sup> Data is a duplicable virtual entity, which by definition is neither tangible nor exclusive. However, a quick examination of today's digital economy reveals that data is de facto treated as if it were a “thing” that can be owned in the same way that goods and chattels are.<sup>132</sup>

According to scholars and practitioners, private laws have historically struggled with managing data as a legal entity.<sup>133</sup> While there are legal provisions that protect and control data, data do not fall neatly and unambiguously into the categories of property and ownership.<sup>134</sup> You can own oil, but not (generally) data. The majority of data sets

---

<sup>128</sup> European Commission, Building A European Data Economy (2017), <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0009&from=EN> (last visited Sep 30, 2021).

<sup>129</sup> For example, in the USA, the debate goes back to the 1960s. See Jessica Litman, Information Privacy/Information Property, 52 *Stanford Law Review* 1283-1313 (2000).

<sup>130</sup> Annie Sorbie et al., Does data ownership hinder biomedical research? Liminal Spaces Policy Brief (2020), <http://Does data ownership hinder biomedical research? Liminal Spaces Policy Brief> (last visited Sep 30, 2021).

<sup>131</sup> E.g., Meglena Kuneva, Keynote Speech, in Roundtable on Online Data Collection, Targeting and Profiling 2 (2009), [https://ec.europa.eu/commission/presscorner/detail/en/SPEECH\\_09\\_156](https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_09_156) (last visited Sep 30, 2021).

<sup>132</sup> Andreas Boerding et al., Data Ownership—A Property Rights Approach from a European Perspective, 11 *JOURNAL OF CIVIL LAW STUDIES* (2018), <https://digitalcommons.law.lsu.edu/jcls/vol11/iss2/5> (last visited Sep 30, 2021).

<sup>133</sup> Wolfgang Kerber, A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis, MAGKS Joint Discussion Paper Series in Economics, No. 37-2016, Philipps-University Marburg, School of Business and Economics (2016), [https://www.uni-marburg.de/fb02/makro/forschung/magkspapers/paper\\_2016/37-2016\\_kerber.pdf](https://www.uni-marburg.de/fb02/makro/forschung/magkspapers/paper_2016/37-2016_kerber.pdf) (last visited Sep 30, 2021).

<sup>134</sup> Patrik Hummel, Matthias Braun & Peter Dabrock, *Own Data? Ethical Reflections on Data Ownership*, 34 *PHILOSOPHY & TECHNOLOGY* 545-572 (2020).

are not protected by copyright. Most data controllers can simulate “real” legal ownership of data by ensuring that “its data” about consumers is legally protectable as trade secrets or confidential information.<sup>135</sup>

Indeed, in light of the growing importance of immaterial assets, there is considerable debate over whether the concept of property should be sufficiently flexible to encompass new objects and rights, to include *res immateriales* (traditionally protected by intellectual property rights)<sup>136</sup>, and to permit data commoditization eventually.<sup>137</sup>

## **4.2 DEFINING PERSONAL, NON PERSONAL DATA, AND MACHINE-GENERATED DATA**

Big data can be generated by humans, machines, or a combination of the two. It can be generated and stored in structured or unstructured formats anywhere information is generated and stored. It can be produced in factories, military units, on the internet, in hospitals, or anywhere else.<sup>138</sup> “Artificial intelligence is expanding its computational capability and utilizing big data techniques to analyze massive datasets in real-time and extract valuable knowledge. As the data-driven transformation spreads throughout society, an ever-increasing amount of data is generated by autonomous, connected machines or Internet of Things-enabled processes (IoT).”<sup>139</sup> This data can be personal data or non-personal data. The debate over who owns data is influenced by the presence of these categories.

“Personal data is the data about a living individual who can be identified. The term 'identifiable' refers to data that can be used to identify an individual, either alone or in

---

<sup>135</sup> Peter Leonard, *Beyond Data Privacy: Data “Ownership” and Regulation of Data-Driven Business* americanbar.org (2020),

[https://www.americanbar.org/groups/science\\_technology/publications/scitech\\_lawyer/2020/winter/beyond-data-privacy-data-ownership-and-regulation-datadriven-business/](https://www.americanbar.org/groups/science_technology/publications/scitech_lawyer/2020/winter/beyond-data-privacy-data-ownership-and-regulation-datadriven-business/) (last visited Sep 30, 2021).

<sup>136</sup> Herbert Zech, *Data as a Tradeable Commodity*, in *EUROPEAN CONTRACT LAW AND THE DIGITAL SINGLE MARKET: THE IMPLICATIONS OF THE DIGITAL REVOLUTION* 51-80 (Alberto De Franceschi 2016), at p 59-60.

<sup>137</sup> Nadezhda Purtova, *The Illusion of Personal Data as No One’s Property*, 7 *LAW, INNOVATION AND TECHNOLOGY* 83-111 (2015); Alberto De Franceschi & Michael Lehmann, *Data as Tradeable Commodity and New Measures for their Protection*, 1 *THE ITALIAN LAW JOURNAL* 51-72 (2015).

<sup>138</sup> Mugdha Ghotkar & Priyanka Rokde, *Big Data: How it is Generated and its Importance*, 2 *IOSR JOURNAL OF COMPUTER ENGINEERING (IOSR-JCE)* 1-5 (2016).

<sup>139</sup> Francesco Banterle, *Data Ownership in the Data Economy: A European Dilemma*, in *EU INTERNET LAW IN THE DIGITAL ERA* (Tatiana-Eleni Synodinou et al. 2020).

conjunction with other data. When determining whether the data can be used in conjunction with other information to identify an individual, it is necessary to consider the means that are reasonably likely to be used to do so.”<sup>140</sup>

Non-personal data can be defined as information about a non-natural person that does not directly or indirectly identify that person, such as<sup>141</sup> general confidential information about businesses, statistical data, and intellectual property assets (e.g., standard essential patents and trade secrets). “Non-personal data also includes anonymous information/data, that is, information that does not pertain to an identified or identifiable natural person or personal data that has been anonymized in such a way that the data subject is no longer identifiable.”<sup>142</sup>

“Machine-generated data is data that is collected, stored, or generated by connected devices, assets, or networks without human intervention. Through an enormous array of connected devices, machine-generated, non-personal data is generated. These devices, which may be geographically dispersed, use their sensors to collect and record a variety of different types of data. A variety of devices can generate non-personal data. Devices may be used in manufacturing processes or as components of street infrastructure, while others may be used to monitor the condition of assets or passenger flows. Additionally, data on the organization, distribution, safety, location, emissions, and network level are examples. All of these have in common that data is generated and collected without human intervention and is aggregated, measured, or stored in such a way that it cannot be used to identify individuals. Machines, which are frequently the same machines that collect non-personal data, can also generate personal data about users, such as their location, health status, or spending habits.”<sup>143</sup>

---

<sup>140</sup> Big Data and Data Protection, <https://rm.coe.int/big-data-and-data-protection-ico-information-commissioner-s-office/1680591220> (last visited Sep 30, 2021).

<sup>141</sup> Michael R. Overly, *Overview of Information Security and Compliance: Seeing the Forest for the Trees*, in *BIG DATA* (James R. Kalyvas & Michael R. Overly 1 ed. 2014).

<sup>142</sup> Recital 26, Official Journal of the European Union | L 119/1 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) (Text with EEA relevance), <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN> (last visited Sep 30, 2021).

<sup>143</sup> Deloitte LLP, *Realising the economic potential of machine-generated, non-personal data in the EU* (2018), [https://www.vodafone.com/content/dam/vodacom/files/public-policy/Realising\\_the\\_potential\\_of\\_IoT\\_data\\_report\\_for\\_Vodafone.pdf](https://www.vodafone.com/content/dam/vodacom/files/public-policy/Realising_the_potential_of_IoT_data_report_for_Vodafone.pdf) (last visited Sep 30, 2021).



### 4.3 PROPERTY RIGHTS IN DATA

Defining 'property' entails striking a balance between the interests of an alleged owner, competing for third-party interests, and public claims to use or have access to the property.<sup>144</sup> Property rights are made up of the right(s) themselves and the object over which the right is asserted (tangible or intangible). However, the content and form of property differ significantly across national legal systems.<sup>145</sup>

“Property rights (ownership) refer to a distinct set of rights in relation to an object. Ownership can be conceptualized as a specific bundle of rights or (in rem) dominium over a thing, depending on the property theory one adheres to.”<sup>146</sup> “The set of ownership rights in the first position includes, but is not limited to, the rights to use, exclude, sell, possess, subdivide, and lease. In the second position, ownership is defined as a relationship between people and a thing that possesses the unilateral characteristic.”<sup>147</sup>

Property rights in information are concerned with identifying a company's or individual's right to control the disclosure, use, alteration, and copying of specified information. The resulting set of rights and limitations includes a declaration of what property exists in information.<sup>148</sup> The potential property rights associated with information include the following<sup>149</sup>:

- Right to data integrity: assurance that information will not be altered or destroyed without the 'owner's consent';<sup>150</sup>

---

<sup>144</sup> Raymond T. Nimmer & Patricia A. Krauthaus, *Information as Property Databases and Commercial Property*, 1 INTERNATIONAL JOURNAL OF LAW AND INFORMATION TECHNOLOGY 3-34 (1993).

<sup>145</sup> Sjeff van Erp, *Ownership of Data: The Numerus Clausus of Legal Objects*, BRIGHAM-KANNER PROPERTY RIGHTS CONFERENCE JOURNAL 235-257 (2017).

<sup>146</sup> Thomas W. Merrill & Henry E. Smith, *What Happened to Property in Law and Economics?*, 111 THE YALE LAW JOURNAL 357 (2001); Robert C. Ellickson, *Two Cheers for the Bundle-of-Sticks Metaphor, Three Cheers for Merrill and Smith*, 8 ECON JOURNAL WATCH 215-222 (2011). See also, J.E. Penner, *The “Bundle of Rights” Picture of Property*, 43 UCLA LAW REVIEW 711-820 (1996).

<sup>147</sup> See, Lisa M. Austin, *The Public Nature of Private Property*, in PROPERTY THEORY: LEGAL AND POLITICAL PERSPECTIVES (James Penner & Michael Otsuka 2018).

<sup>148</sup> Nimmer & Krauthaus, *supra* note 144.

<sup>149</sup> *Id.*

<sup>150</sup> *Id.*

- Right to use data: the capability of an individual or organization to use the information for internal purposes such as business guidance, technology development, and marketing;<sup>151</sup>
- Right to data disclosure: the right to make broad or selective disclosures of information or to decline to do so;<sup>152</sup>
- Right to copy data: the right to reproduce the information in written or other tangible forms;<sup>153</sup>
- Right to data access control: the owner's right to restrict access to information known to him.<sup>154</sup>

With property rights comes the ability to negotiate with firms about what uses of your personal information you are willing to allow and for how much.<sup>155</sup> “They would be compensated for the expected privacy cost associated with each information disclosure if they owned their personal data.”<sup>156</sup>

Property rights in data are seen as supporting industry investment in data collection, data creation, and generation. Some see a property rights basis for individual control over personal information as a bulwark against the unauthorized collection and use of personal information from a data protection standpoint.<sup>157</sup>

#### 4.4 DATA OWNERSHIP AND CONTROL OVER DATA

---

<sup>151</sup> *Id.*

<sup>152</sup> *Id.*

<sup>153</sup> *Id.*

<sup>154</sup> *Id.*

<sup>155</sup> Kenneth C. Laudon, Markets and Privacy, 39 Communications of the ACM 92-104 (1996); Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381, 2413 (1996); Lawrence Lessig, *The Architecture of Privacy: Remaking Privacy in Cyberspace*, 1 VANDERBILT JOURNAL OF ENTERTAINMENT AND TECHNOLOGY LAW 56-65 (1999); Patricia Mell, *Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness*, 11 BERKELEY TECHNOLOGY LAW JOURNAL 1-92 (1996); Lawrence Lessig, Code And Other Laws of Cyberspace 85-90 (1 ed. 1999); Jamie Lund, *Property Rights to Information*, 10 NORTHWESTERN JOURNAL OF TECHNOLOGY AND INTELLECTUAL PROPERTY 1-18 (2011); Jane B. Baron, Property as Control: The Case of Information, 18 MICHIGAN TELECOMMUNICATIONS AND TECHNOLOGY LAW REVIEW 367-418 (2012); Jim Harper, Perspectives on property rights in data [www.aei.org](http://www.aei.org) (2019), <https://www.aei.org/technology-and-innovation/perspectives-on-property-rights-in-data/> (last visited Sep 30, 2021).

<sup>156</sup> Corien Prins, When personal data, behavior and virtual identities become a commodity: Would a property rights approach matter?, 3 SCRIPT-ed 270-303 (2006) at 271.

<sup>157</sup> Teresa Scassa, Data Ownership, CIGI Paper No. 187 (2018), <https://www.cigionline.org/publications/data-ownership/> (last visited Sep 30, 2021).

“Ownership is a fundamental concept that pervades our daily lives and fundamental social mechanisms.”<sup>158</sup> It refers to the delegation of property rights and responsibilities to an individual or an organization. Three distinct types of rights are discernible: the rights to use, the rights to control, and the rights to remain in control.<sup>159</sup>

In terms of philosophical assumptions, various theories enable the emergence and assignment of ownership to be explained<sup>160</sup>:

- According to Immanuel Kant's first occupancy theory, the property is assigned to the first person who possesses it.
- According to John Locke's labour theory, ownership is determined by the amount of value-added through labour.
- According to Jeremy Bentham's and John Stuart Mill's utility theory, ownership is assigned in such a way that the benefits to all parties involved are maximized.
- According to Robert Nozick's and John Rawls's libertarian theory, ownership must be distributed in such a way that it does not impair others' ability to act autonomously.
- According to Georg Wilhelm Friedrich Hegel's personality theory, ownership is determined by a person's desire to invest in an object, which qualifies them as its owner.

These varying perceptions of ownership exist for data as well, but they must take into account data's inherent characteristics, such as nonrivalrousness.<sup>161</sup>

“Ownership confers complete discretion on the right holder regarding the exercise of the right (i.e., the right to exploit, change, destroy, and obtain benefits that an owned asset can generate). Allocation of ownership rights has a wide range of consequences: Ownership provides the right holder with absolute protection, i.e., the rights can be exercised and enforced against anyone, not just contractual parties. It is a widespread misconception that the owner of a data-generating device (for example, a mobile phone

---

<sup>158</sup> Andrei Shleifer, *State versus Private Ownership*, 12 JOURNAL OF ECONOMIC PERSPECTIVES 133-150 (1998).

<sup>159</sup> Dennis Hart, *Ownership as an Issue in Data and Information Sharing: A Philosophically Based Review*, 10 AUSTRALASIAN JOURNAL OF INFORMATION SYSTEMS (2002).

<sup>160</sup> *Id.*

<sup>161</sup> Martin Fadler & Christine Legner, *Who Owns Data in the Enterprise? Rethinking Data Ownership in times of Big Data and Analytics*, in 28th European Conference on Information Systems (ECIS) (2020).

user or a car driver) or the manufacturer of the device (for example, a mobile phone manufacturer or a car manufacturer) can legally “own” data. Only by law can ownership rights be recognized and established. However, no such 'data ownership right' exists at the EU or Member State level or in any other developed country.”<sup>162</sup>

According to the law, ownership is the most comprehensive right that a person can have over an object. Moreover, things are tangible objects that humans can manipulate. As a result, this concept does not apply to data.<sup>163</sup>

“Data ownership is not a matter of ownership in the traditional sense. It all comes down to consent and control. When people talk about data ownership, they refer to data protected by a property rule, not to actual ownership rights in data. This is evident in the literature's language and the emphasis placed on consent.”<sup>164</sup> “All data ownership proposals seek to give people control over their personal information by allowing them to decide when to give it away and how much to expect to be paid for it. As it turns out, this is all about trade, not ownership.”<sup>165</sup>

Numerous discussions about data propertization conflate data ownership with control over data. While these terms may have a similar colloquial meaning, they confer a very different set of rights and responsibilities on individuals when applied in a legal context.<sup>166</sup>

“The majority of policy proposals supporting treating data ownership or privacy as property relies on consent as a mechanism for authorizing the surrender of privacy. These proposals propose that data subjects' rights to their personal information (privacy rights) should not be transmitted without their consent and in exchange for a socially

---

<sup>162</sup> Max Competition, Arguments Against “Data Ownership” - Max Planck Institute for Innovation and Competition Max Planck Institute for Innovation and Competition, [https://www.ip.mpg.de/fileadmin/ipmpg/content/forschung/Argumentarium-Dateneigentum\\_eng.pdf](https://www.ip.mpg.de/fileadmin/ipmpg/content/forschung/Argumentarium-Dateneigentum_eng.pdf) (last visited Sep 30, 2021).

<sup>163</sup> Lora Mourcous, Ownership of Personal Data under Dutch law? SOLV (2020), <https://solv.nl/en/blog/ownership-of-personal-data-in-dutch-law/> (last visited Sep 30, 2021).

<sup>164</sup> Ignacio Cofone, *Beyond Data Ownership*, 43 CARDOZO LAW REVIEW, [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3564480&download=yes](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3564480&download=yes).

<sup>165</sup> *Id.*

<sup>166</sup> William R. Vance, *The Restatement of the Law of Property*, 86 UNIVERSITY OF PENNSYLVANIA LAW REVIEW AND AMERICAN LAW REGISTER 173 (1937); HENRY CAMPBELL BLACK, OWNERSHIP BLACK'S LAW DICTIONARY (10 ed. 2009).

determined compensation, but rather with their consent and in exchange for a bargained-for compensation.”<sup>167</sup>

“The majority of academic and policy debates about data ownership do not refer to ownership. They are referring to property rules. This is because, like those who advocate for data as property, they do not discuss the nature of an entitlement (right) but rather how that entitlement is transferred in the marketplace—and whether there should be one at all. For example, van den Hoven examines ownership as a means of maximizing data subjects' control over their personal information,<sup>168</sup> despite the fact that the type of entitlement confers little control on the holder—it is the transfer rules that confer control.”<sup>169</sup>

Property rules are distinct from ownership—which is erroneously referred to as property rights. A property rule protects rights that can only be transferred with the consent of the title-holder and for a price determined through negotiation.<sup>170</sup> Ownership rights (or property rights) are a type of right that can be protected by any type of transfer rule: property, liability, or inalienability. On the other hand — and this is an unfortunate ambiguity — property rules are a consent-based transfer rule that can be applied to any type of right.<sup>171</sup>

Consent is governed by property rules. In general, “when viewed as a critical mechanism for ensuring privacy, informed consent is a natural corollary of the notion that privacy entails control over one's own information.”<sup>172</sup> The consent-based argument defends the use of property rules to govern the collection, processing, and distribution of people's personal information, which is collected, processed, and distributed primarily with their consent.<sup>173</sup>

---

<sup>167</sup> Cofone, *supra* note 164.

<sup>168</sup> Jeroen van den Hoven et al., Privacy and Information Technology, in *Stanford Encyclopedia of Philosophy* (Edward N. Zalta 2019), <https://plato.stanford.edu/archives/win2019/entries/it-privacy/> (last visited Sep 30, 2021).

<sup>169</sup> Cofone, *supra* note 164.

<sup>170</sup> Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 *HARVARD LAW REVIEW* 1089 (1972), at 1106.

<sup>171</sup> Cofone, *supra* note 164.

<sup>172</sup> Solon Barocas & Helen Nissenbaum, *Big Data's End Run around Anonymity and Consent*, in *PRIVACY, BIG DATA, AND THE PUBLIC GOOD* 44-75 (Julia Lane et al. 2014).

<sup>173</sup> Cofone, *supra* note 164.

Many privacy-related legislative developments over the last few decades have included the right to control. For example, laws governing data consent allow individuals to control their own data by limiting its use and dissemination while allowing businesses to use the same data for both business and consumer benefit. As stated previously, “control” is distinct from “ownership.” While an individual may have the ability to control data, this does not always imply that he or she also has the ability to exercise the other rights and responsibilities associated with ownership. Indeed, the characteristics of consumer data make granting individuals a traditional property right in their data surprisingly difficult.<sup>174</sup>

While individuals have the ability to restrict the use of their personal data, these restrictions demonstrate “control” but do not amount to ownership. Individuals currently do not “own” their own data.<sup>175</sup>

“This control is not and cannot be unlimited. For example, a citizen has limited control because the government needs this information to carry out its legal duties. These data must be accurate, current, available, and reliable. As a result, a citizen cannot, for example, refuse to have his or her name, address, and date of birth recorded by the government.”<sup>176</sup>

“Today, the vast majority of data is generated by a handful of technologies that consumers use on a daily basis. As a result, the brands that own those assets/systems/apps — Apple, Amazon, Facebook, Google, and Microsoft, for example — control the lion's share of global customer data.”<sup>177</sup> The majority of personal data is collected and stored by businesses, either by businesses that provide various services to individuals or by data brokers rather than by data subjects.<sup>178</sup> Thus, while these

---

<sup>174</sup> Thomas M. Boyd & Tara Sugiyama Potashnik, *Data Ownership - The Suitability of a Consumer Property Right in a 21st Century Economy* (2020), <https://www.venable.com/insights/publications/2020/09/data-ownership> (last visited Sep 30, 2021).

<sup>175</sup> Lothar Determann, *No One Owns Data*, 70 HASTINGS LAW JOURNAL 1-44 (2019), at 38-39.

<sup>176</sup> *Supra* note 163.

<sup>177</sup> Carine Alexis, *The Future of Data: Ownership, Application, AI, and New Roles* Movableink.com (2018), <https://movableink.com/blog/the-future-of-data-ownership-application-ai-and-new-roles> (last visited Sep 30, 2021).

<sup>178</sup> To justify their ownership of customer personal data, technology companies assert that they have invested heavily in developing their business models and developing sophisticated tools for harnessing customer data. For one example, see Equifax CEO Mark Begor's testimony to the US House of Representatives, in which he explains that Equifax always strives to have the most current and relevant data about their customers. See generally, Mark Begor, *Written Testimony, in Hearing: Who's Keeping Score? Holding Credit Bureaus Accountable and Repairing a Broken System*, Committee on Financial

companies do not legally own data, they can be considered de facto owners of data (owners in an economic sense).<sup>179</sup> The companies enjoy control over the data, and it is that control individuals want to themselves when they demand data ownership.

#### 4.5 MULTIPLE STAKEHOLDERS IN DATA

Data are often a subject with multiple interests. Even with personal data, it is possible to imagine competing interests. For example, one could argue that a person's medical history, including DNA, is also their children's personal information. Ownership rights appear to be a blunt instrument for resolving conflicting interests. Across all contexts, issues would arise. Consider the interests of the company collecting personal information and the interests of the individuals whose personal information is collected. Is the right based on the information's source or the resources invested in defining and harvesting it? How do you balance the interests of a company that supplies the hardware that captures data, a company that derives data from the captured data, a city that allows access to its streets and spaces to collect data? Creating a new right would necessitate advance planning. It would also necessitate consideration of users' rights and the public's interest in data access and use.<sup>180</sup>

While ownership rights to physical property are binary, those to data are layered and thus difficult to determine. In the case of personal data, 'data principals,' that is, individuals whose personal information is collected and processed, can demonstrate ownership by exerting control over how their personal data is used. As a result, data principals are recognized as the owners of their personal data under data protection laws. The Committee recognizes that in the case of non-personal data (NPD), an

---

Services U.S. House of Representatives (2019), <https://docs.house.gov/meetings/BA/BA00/20190226/108945/HHRG-116-BA00-Wstate-BegorM-20190226.pdf> (last visited Sep 30, 2021).

<sup>179</sup> Nestor Duch-Brown, Bertin Martens & Frank Mueller-Langer, *The Economics of Ownership, Access and Trade in Digital Data* (2017), at 23–24. <https://ec.europa.eu/jrc/sites/default/files/jrc104756.pdf> (last visited Sep 30, 2021).

<sup>180</sup> Teresa Scassa, *Sharing Data in the Platform Economy: A Public Interest Argument for Access to Platform Data*, 50 UBC LAW REVIEW 1017-1071 (2017).

individual ownership approach is impractical due to the lack of identifiable data principals.<sup>181</sup>

Individuals as data subjects are increasingly asserting their ownership of data (subject as owner). The concept of data ownership becomes more complex in the context of organizations (enterprise as owner) due to distributed data creation and processing within organizations. Three distinct grounds for claiming ownership can be identified here. To begin, organizations assert ownership based on monetary considerations such as funding (funding organization as owner) or data acquisition/licensing (purchaser/licensor as owner). These paradigms are always two-sided. On the one hand, the organization that funds the data creator; on the other hand, the organization that purchases or licenses another party's data. While the first case involves the transfer of data ownership without restriction to the funding organization, in the second case, data ownership is transferred with certain restrictions to the purchasing/licensing party. Second, an organization may assert ownership through the use of data. This is frequently the case for consuming parties (consumers as owners) who require high confidence in the data and thus assume responsibility. Additionally, it may apply to parties that read data from various sources (reader as owner) in order to create or add to their knowledge base. Thirdly, organizations derive value from data processing and thus assert ownership. Four paradigms can be distinguished according to the type of processing: data creation (creator as owner), data formatting (packager as owner), data compilation from various data sources (compiler as owner), and data decoding (decoder as owner).<sup>182</sup>

Due to the complexity of the “data value chain,” the issue of data ownership is made even more difficult. Indeed, the data ecosystem in big data and IoT is characterized by the interactions of multiple actors and operations. Various stakeholders may act at varying levels during the data creation and generation processes. They can utilize, compile, create, select, structure, enrich, analyze, and add value to data, for example.

---

<sup>181</sup> The Ministry of Electronics & Information Technology (MeitY), Report by the Committee of Experts on Non-Personal Data Governance Framework (2020), <https://ourgovdotin.files.wordpress.com/2020/12/revised-report-kris-gopalakrishnan-committee-report-on-non-personal-data-governance-framework.pdf> (last visited Sep 30, 2021).

<sup>182</sup> Marshall Van Alstyne, Erik Brynjolfsson & Stuart Madnick, *Why Not One Big Database? Principles for Data Ownership*, 15 DECISION SUPPORT SYSTEMS 267-284 (1995); Martin Fadler & Christine Legner, Who Owns Data in the Enterprise? Rethinking Data Ownership in times of Big Data and Analytics, in 28th European Conference on Information Systems (ECIS) (2020).



As a result, determining who is entitled to claim ownership of data may be difficult, as each of these actors may claim ownership at a different level, depending on their specific role. No single actor is likely to have exclusive rights.<sup>183</sup> Who owns the data can become complicated with multiple claimants. As more sources are aggregated, the situation becomes more complicated.<sup>184</sup>

Different approaches to regulating the ownership of data are being discussed at the moment are<sup>185</sup>:

- “Data-specific approach: This approach would entail categorizing data ownership according to the type of data. The type of data determines whether it is owned by an individual or a business, according to this approach. For example, if data is associated with a business (e.g., machine data), it is owned by the business rather than by the individual to whom the data pertains.”<sup>186</sup>
- “Property law approach: The ownership of data can be classified according to how and where it is stored. This approach imparts a sense of 'tangibility.' However, because data's primary value is in its portability and businesses are increasingly storing their data in cloud systems, this approach may fall short of adequately addressing data as an asset class.”<sup>187</sup>
- “Action-related approach: A different approach is to grant data ownership to the data producer. This model also introduces uncertainty; for example, who would be the “producer of the data”: (i) the individuals to whom the data pertains, (ii) the data compiler, or (iii) someone else?”<sup>188</sup>
- “Beneficial owner approach: An alternative approach is that involves data being assigned to a “beneficial owner.” According to this approach, ownership of data would be determined by taking into account factors such as the “merit” of data generation, production costs, and additional costs associated with data storage.

---

<sup>183</sup> Banterle, *supra* note 139.

<sup>184</sup> Who owns the Machine Generated Data in IoT – Men or Machine?, IIoT World (2017), <https://www.iiot-world.com/industrial-iot/digital-disruption/who-owns-the-machine-generated-data-in-iiot-men-or-machine/> (last visited Sep 30, 2021).

<sup>185</sup> Claudia Milbradt, Global Intellectual Property Newsletter –23rd Edition – Legal Issues Surrounding the Protection of 'Data' and other IP Topics, Clifford Chance (2019), <https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2019/09/global-intellectual-property-newsletter-23rd-edition-legal-issues-surrounding-the-protection-of-data-and-other-ip-t.pdf> (last visited Sep 30, 2021).

<sup>186</sup> *Id.*

<sup>187</sup> *Id.*

<sup>188</sup> *Id.*

However, given the exponential growth of data production and storage, as described above, this approach would almost certainly result in numerous disputes between the various parties who have borne costs associated with the data.”<sup>189</sup>

Granting (exclusive) data ownership rights to specific categories of stakeholders may not be the optimal course of action. Apart from posing significant competition risks, data ownership would almost certainly be extremely difficult to regulate. For instance, determining rightholdership is not always straightforward, as multiple stakeholders frequently contribute directly or indirectly to data collection and processing. Additionally, potential data co-ownership could result in blocking situations<sup>190</sup> and exacerbate inefficiencies caused by data underuse. Indeed, a complex system of exceptions and limitations would have to be implemented, taking other subjects' interests into account.<sup>191</sup>

#### **4.6 CONSEQUENCES OF DATA OWNERSHIP**

If a property right in data is granted, the ability to exercise control is likely to erode. When a consumer's property right is sold, the consumer relinquishes his or her ownership rights and ability to exercise control over the property.<sup>192</sup>

If individuals have a property right in their personal data, data required for research may become less accessible as a result of the cost of obtaining the necessary data and/or the data owners' decision to withhold the data. The cost of data collection may be prohibitively expensive for researchers, forcing them to conduct research using smaller datasets and sample sizes. With smaller datasets and sample sizes, such studies will be less reliable, and scientific progress will be slowed, which will have a particularly negative impact on healthcare.<sup>193</sup>

---

<sup>189</sup> *Id.*

<sup>190</sup> Cf. Josef Drexl et al., Position Statement of the Max Planck Institute for Innovation and Competition of 26 April 2017 on the European Commission's 'Public consultation on Building the European Data Economy', Max Planck Institute for Innovation & Competition Research Paper No. 17-08 (2017), at 7-8.

<sup>191</sup> *Id.* at 9–10.

<sup>192</sup> Barocas & Nissenbaum, *supra* note 172.

<sup>193</sup> *Id.*

Creating a property right in data may also have a detrimental effect on people with limited resources. For example, individuals with more resources may be less willing to sell data to businesses, which may result in skewed data sets collected by businesses but also, and perhaps more importantly, may result in the application of privacy protections based on economic status. A data property right could serve as a mirror image of a pay-for-privacy (PFP) model. Consumers can pay for increased privacy restrictions through PFP models.<sup>194</sup>

Several of the world's largest companies have business models that are heavily reliant on data.<sup>195</sup> If there is a data property right, the costs of entry into such a market may become prohibitively high.

“Transaction costs would almost certainly increase significantly, as contracting parties would need to clarify whether the parties exercising control over data are also authorized to grant access to third parties acting as potential 'data owners.' Additionally, establishing 'data ownership rights' may result in imbalances in the bargaining positions of the contracting parties, particularly if 'data ownership' is assigned to the contracting party that is already superior. Additionally, the introduction of 'data ownership rights' would necessitate the formulation of comprehensive exceptions to safeguard against unjustified competition restraints. This would increase the likelihood of protracted judicial disputes. Rather than promoting the digital economy and facilitating data access, not least in the public interest, introducing 'data ownership rights' would have the exact opposite effect.”<sup>196</sup>

## 4.7 CONCLUSION

---

<sup>194</sup> Adam Schwartz, The Payoff From California’s “Data Dividend” Must Be Stronger Privacy Laws Electronic Frontier Foundation (2019), <https://www.eff.org/deeplinks/2019/02/payoff-californias-data-dividend-must-be-stronger-privacy-laws> (last visited Sep 30, 2021).

<sup>195</sup> Amazon, Alphabet (Google), and Facebook all use data about consumers to offer services. See Mark Hall, Amazon.com | History & Facts Encyclopedia Britannica, <https://www.britannica.com/topic/Amazoncom> (last visited Sep 30, 2021); see Policies.google.com, <https://policies.google.com/technologies/partner-sites?hl=en-US> (last visited Sep 30, 2021); see, Mark Hall, Facebook | Overview, History, & Facts Encyclopedia Britannica (2021), <https://www.britannica.com/topic/Facebook> (last visited Sep 30, 2021).

<sup>196</sup> Hart, *supra* note 159.

Existing frameworks protect a de facto “possession” rather than a concept of “ownership.” In the absence of a comprehensive property regime applicable to data as a whole, raw data is primarily controlled through contractual and access restriction mechanisms based on factual exclusivity and without recognition of ownership in the private law sense.<sup>197</sup>

“The issue of data ownership is inextricably linked to the relationship between privacy protection and informational self-determination on the one hand and freedom of thought, communication, science, economic competition, and technological innovation on the other. Data has so far been unprotected by a proprietary right to protect both types of interests.”<sup>198</sup>

Nonetheless, the mere fact that a piece of data is associated with a particular individual does not imply that the individual also legally “owns” their personal data.<sup>199</sup> Indeed, current data protection laws make no distinction between who owns personal data and who does not.<sup>200</sup> Additionally, no other legal principle or theory justifies the allocation of exclusive property rights over data on its own.<sup>201</sup> For this reason, any recognition of a new (intellectual) property right, like a right to own data, would need to be justified.<sup>202</sup> Such a justification does not exist at the moment.<sup>203</sup>

---

<sup>197</sup> Banterle, *supra* note 139.

<sup>198</sup> *Supra* note 185.

<sup>199</sup> Josef Drexl, *Designing Competitive Markets for Industrial Data - Between Propertisation and Access*, 8 JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law 257-292 (2016).

<sup>200</sup> See, *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*, Directorate for Science, Technology and Innovation, OECD Publishing, Paris (2019). Cf. Nestor Duch-Brown, Bertin Martens & Frank Mueller-Langer, *The Economics of Ownership, Access and Trade in Digital Data* (2017).

<sup>201</sup> Josef Drexl et al., *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 & Competition Research Paper No. 16-10 (2016).

<sup>202</sup> Cf. Josef Drexl et al., *Position Statement of the Max Planck Institute for Innovation and Competition of 26 April 2017 on the European Commission's 'Public consultation on Building the European Data Economy'*, Max Planck Institute for Innovation & Competition Research Paper No. 17-08 (2017); For personal data ownership rationales and their flaws, see, Václav Janeček, *Ownership of personal data in the Internet of Things*, 34 COMPUTER LAW & SECURITY REVIEW 1039-1052 (2018).

<sup>203</sup> Václav Janeček concludes in his analysis of the concept of data ownership's applicability in the IoT context that, at the moment, neither a top-down nor a bottom-up approach justifies the introduction of ownership rights in personal data. The top-down approach falls short of convincingly demonstrating why ownership-like control is the best model of data control for achieving economic and factual goals. On the other hand, for the bottom-up approach to work, (1) enhanced factual control over data by the potential rightholder is required, and (2) regardless of the approach taken, it is implausible to expect that the law will provide stable protection for personal data because existing IoT architectures are insufficiently transparent. Václav Janeček, *Ownership of personal data in the Internet of Things*, 34

# CHAPTER V:

## PROTECTION OF DATA IN CONNECTION WITH CROSS BORDER DATA TRANSFERS

### 5.1 INTRODUCTION

Today's trade is inextricably linked to the movement of data across borders, either as part of the transaction or as the product itself.<sup>204</sup> “It is widely recognized that data has a monetary value that transcends borders and industries. The value, however, is distinct from that assigned to physical commodities such as oil.”<sup>205</sup> In the words of the Swedish National Board of Trade, “in order to conduct business, companies must exchange data with one another.”<sup>206</sup>

“The data movement is what underpins digital commerce. Not only is data a means of production, but it is also a tradable asset and a mechanism for the organization of GVCs and the delivery of services. It also indirectly supports physical trade by enabling trade facilitation to be implemented. Additionally, data is critical to the development and rapid expansion of emerging and rapidly expanding service delivery models such as cloud computing, the Internet of Things (IoT), and additive manufacturing.”<sup>207</sup>

The information economy facilitates the movement of large amounts of digitized information and data across national borders. Global GDP increased by approximately

---

COMPUTER LAW & SECURITY REVIEW 1039-1052 (2018), at 1044–46. On the other hand, Nadezhda Purtova argues that the introduction of personal data ownership rights would provide ultimate clarity regarding the allocation of data protection obligations. NADEZHDA PURTOVA, PROPERTY RIGHTS IN PERSONAL DATA: A EUROPEAN PERSPECTIVE (2011).

<sup>204</sup> The OECD Privacy Framework, (2013), [https://www.oecd.org/sti/ieconomy/oecd\\_privacy\\_framework.pdf](https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf)

<sup>205</sup> See, Michael Mandel, *The Economic Impact of Data: Why Data Is Not Like Oil* (2017). [https://www.progressivepolicy.org/wp-content/uploads/2017/07/PowerofData-Report\\_2017.pdf](https://www.progressivepolicy.org/wp-content/uploads/2017/07/PowerofData-Report_2017.pdf)

<sup>206</sup> See, L. Lee Tuthill, *Cross-Border Data Flows: What Role for Trade Rules?*, in RESEARCH HANDBOOK ON TRADE IN SERVICES 357–382 (Pierre Sauvé & Martin Roy 1 ed. 2016).

<sup>207</sup> Digital trade - OECD, Oecd.org, <https://www.oecd.org/trade/topics/digital-trade/> (last visited Sep 29, 2021).

10%, or \$7.8 trillion, in 2014, as a result of international trade in goods, services, and finance. Data flows account for approximately \$2.8 trillion of this additional value.<sup>208</sup>

“International businesses now manage customer data in a variety of ways. Governments in a variety of countries have expressed concern about these cross-border data flows. One significant concern is the possibility of personal information being compromised. For instance, in 2005, undercover reporters from the Australian Broadcasting Corporation were allegedly offered for sale the personal information of 1,000 Australians for around US\$10 per person.”<sup>209</sup> Individuals are now willingly disclosing personal information in exchange for online services.<sup>210</sup>

“As data's role in society has grown and intensified, the interfaces between trade and privacy protection have grown and intensified, raising critical questions about how to design an appropriate regulatory framework that balances economic and non-economic concerns, as well as national and international interests.”<sup>211</sup>

However, the misuse of personal data is likely to jeopardize fundamental human values. To ensure economic, social, and cultural development, it is necessary to ensure that economic considerations do not trump human rights and fundamental freedoms. The balance of these disparate elements is typically managed through national sectoral legislation and international treaties. Even so, national court judgments are critical in interpreting and applying data protection rules: the balance *verbo tenus* must therefore be applied to each specific case, with additional and distinct shades that are not readily foreseeable *ex-ante*.<sup>212</sup>

---

<sup>208</sup> James Manyika et al., *Digital Globalization: The New Era of Global Flows* (2016), <https://www.mckinsey.com/~media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20globalization%20The%20new%20era%20of%20global%20flows/MGI-Digital-globalization-Full-report.ashx> (last visited Sep 29, 2021).

<sup>209</sup> See, Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (2008), <https://www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/31-cross-border-data-flows/introduction-139/> (last visited Sep 29, 2021).

<sup>210</sup> Adrienn Lukács, *What Is Privacy? The History and Definition of Privacy* (2016), <http://publicatio.bibl.u-szeged.hu/10794/7/3188699.pdf> (last visited Sep 29, 2021).

<sup>211</sup> Mira Burri, *Interfacing Privacy and Trade*, 53 *Case W. Res. J. Int'l L.* 35 (2021), 53 *CASE WESTERN RESERVE JOURNAL OF INTERNATIONAL LAW* (2021), <https://scholarlycommons.law.case.edu/cgi/viewcontent.cgi?article=2596&context=jil> (last visited Sep 29, 2021).

<sup>212</sup> Davide Borelli, *International Trading of Big Data*, 3 *ATHENS JOURNAL OF LAW* 21-30 (2016).

“The international framework for privacy has evolved over time, in part as a result of the effects of new technologies and the new threats they may pose to data protection.”<sup>213</sup> Internationally, the United Nations adopted a series of resolutions addressing “the right to privacy in the digital age.” The *Revised draft resolution on the right to privacy in the digital age*<sup>214</sup> states unequivocally that “the increasing capability of business enterprises to collect, process, and use personal data may jeopardize the enjoyment of the right to privacy in the digital age.” Additionally, it notes that states are required to “take effective measures to prevent the unauthorized retention, processing, and use of personal data stored by public authorities and business enterprises.” UN resolutions, despite their non-binding nature, are regarded as strong evidence of state practice and opinion juris.

Domestic data protection legislation is becoming increasingly prevalent throughout the world. According to UNCTAD's Global Database of Data Protection and Privacy Legislation, 107 countries have enacted legislation to safeguard data and privacy, 66 of which are developing countries. Currently, 10% of countries are in the process of drafting. The remainder either lack legislation or lack data.<sup>215</sup>

According to a study conducted among Data Protection Laws of 71 countries, around 55 countries require prior consent, while ten require an obligation to inform; around 39 countries have enacted legislation (commonly known as Data Breach Notification Law) requiring notification of data breaches; Data Protection Authorities exist in 58 countries; only 17 countries have Data Protection Laws that necessitate the appointment of a Data Protection Officer; only five countries impose a maximum penalty of one million euros for non-compliance with Data Protection Laws, and around 35 countries have made non-compliance with the Data Protection Laws a criminal offence.<sup>216</sup>

---

<sup>213</sup> See, Oliver Diggelmann & Maria N. Cleis, *How The Right To Privacy Became A Human Right*, 14 HUM. RTS. L. REV. 441, 446–47 (2014), <https://www.corteidh.or.cr/tablas/r33348.pdf>

<sup>214</sup> UN, GENERAL ASSEMBLY, REVISED DRAFT RESOLUTION ON THE RIGHT TO PRIVACY IN THE DIGITAL AGE, A/C.3/71/L.39/ REV.1, NEW YORK, 16 NOVEMBER 2016, [https://digitallibrary.un.org/record/848969/files/A\\_C-3\\_71\\_L-39\\_Rev-1-EN.pdf](https://digitallibrary.un.org/record/848969/files/A_C-3_71_L-39_Rev-1-EN.pdf); UN, HUMAN RIGHTS COUNCIL, THE RIGHT TO PRIVACY IN THE DIGITAL AGE (2017), A/HRC/34/L.7/REV.1, <https://documents-dds-ny.un.org/doc/UNDOC/LTD/G17/073/06/PDF/G1707306.pdf?OpenElement>.

<sup>215</sup> UNCTAD, Data Protection and Privacy Legislation Worldwide, unctad.org, <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide> (last accessed Sep 29, 2021).

<sup>216</sup> See, Bernold Nieuwesteeg, Quantifying Key Characteristics of 71 Data Protection Laws, 7 *Journal of Intellectual Property, Information Technology and E-Commerce Law* (2016), <https://www.jipitec.eu/issues/jipitec-7-3-2016>.

The growing concern about the right to data protection is closely related to its fundamental status, which is enshrined in a variety of constitutional instruments either as a distinct right or as a necessary component of the right to privacy.<sup>217</sup> Among countries or regions with data protection laws, the EU and the US are regarded as critical players due to their dominance in digital commerce.<sup>218</sup>

The study is limited to and concerned with the data protection policies of various jurisdictions in relation to cross-border data flows.

## **5.2 INTERNATIONAL AND NATIONAL LEGAL FRAMEWORKS CONCERNING DATA PROTECTION AND CROSS BORDER DATA TRANSFERS**

### **5.2.1 ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT**

“The OECD was the first organization to endorse privacy principles, recognizing both the importance of facilitating cross-border data flows as a foundation for economic and social development and the risks associated with them.”<sup>219</sup> “OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (“OECD Guidelines”)<sup>220</sup> sought to achieve this balance by (1) establishing certain fundamental principles for the national and international application that allowed for legitimate restrictions while maintaining free data flows, and (2) providing a framework for national implementation and international cooperation.”<sup>221</sup> “The OECD Guidelines uphold eight principles that

---

<sup>217</sup> Zhen Zhang, Personal Data Protection within WTO’s Trade Framework. <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEWjVzInx5aPzAhXn93MBHRA9Cf4QFnoECAIQAQ&url=https%3A%2F%2Fscripties.uba.uva.nl%2Fdownload%3Ffid%3Dc1413888&usg=AOvVaw00r65tbH5iWUVDzaI0PAhP> (last accessed Sep 29, 2021)

<sup>218</sup> *Id.*

<sup>219</sup> See, e.g., OECD (2011-04-06), “The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines”, OECD Digital Economy Papers, No. 176, OECD Publishing, Paris. <http://dx.doi.org/10.1787/5kgf09z90c31-en>

<sup>220</sup> OECD Guidelines On the Protection of Privacy and Transborder Flows of Personal Data (23 September 1980).

<https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprivacyandtransborderflowsofpersonaldata.htm>.

<sup>221</sup> *Id.*



apply to both the public and private sectors and encourage countries to develop their own privacy protection frameworks in accordance with them.”<sup>222</sup> These eight principles are as follows: (1) collection limitation; (2) data quality; (3) purpose specification; (4) use limitation; (5) the principle of security safeguards; (6) openness; (7) individual participation; and (8) accountability.<sup>223</sup> These principles have become integral components of all subsequent national data protection regimes, including the EU framework.

“The OECD Guidelines were revised in 2013,<sup>224</sup> which introduced a number of new concepts, including national privacy strategies, privacy management programs, and data security breach notification, that allow for implementation flexibility while also acknowledging newer demands from governments to approach data protection as an increasingly critical issue.”<sup>225</sup>

## **5.2.2 ASIA-PACIFIC ECONOMIC COOPERATION**

The APEC Privacy Framework was created in 2015 to promote electronic commerce throughout the Asia-Pacific region. It is consistent with the 2013 OECD Privacy Guidelines.<sup>226</sup> This framework includes principles to protect personal data. However, it gives more freedom for the transfer of data than the OECD Guidelines.

The APEC Privacy Framework “encourages Members to avoid the creation of unnecessary barriers to information flows.”<sup>227</sup> The APEC Privacy Framework promotes cross-border cooperation among members. These may include mechanisms to aid in investigations and identify and prioritize cases for cooperation in serious cases of privacy infringement.<sup>228</sup>

The framework includes privacy principles. Because of the similarities with the OECD Guidelines, it is not necessary to repeat all of them. APEC Principle 9 is critical. It states

---

<sup>222</sup> Burri, *supra* note 211.

<sup>223</sup> *Id.*

<sup>224</sup> The OECD Privacy Framework, [C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79], [https://www.oecd.org/sti/ieconomy/oecd\\_privacy\\_framework.pdf](https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf)

<sup>225</sup> Burri, *supra* note 211.

<sup>226</sup> APEC Privacy Framework (2015). [https://www.apec.org/-/media/APEC/Publications/2017/8/APEC-Privacy-Framework-\(2015\)/217\\_ECSG\\_2015-APEC-Privacy-Framework.pdf](https://www.apec.org/-/media/APEC/Publications/2017/8/APEC-Privacy-Framework-(2015)/217_ECSG_2015-APEC-Privacy-Framework.pdf)

<sup>227</sup> *Id.*

<sup>228</sup> *Id.* principle 5.

that “accountability should follow the data.”<sup>229</sup> According to Crompton and Ford, “the most significant difference between the APEC Framework and the EU Directive on border controls is this principle.”<sup>230</sup> According to the Framework, once an organization collects personal information, it is responsible for the data “whether domestically or internationally.”<sup>231</sup> This principle is important because it is based on the protection of the data and the parties to it, the person and the collector. The framework does not impose a cross-border barrier to the transfer of personal data.

Some have argued that the framework is too weak in terms of privacy protection. For example, Professor Graham Greenleaf contends that it favours the free flow of personal information.<sup>232</sup> The requirement of accountability, combined with a requirement of consent or that the disclosed takes reasonable steps to protect the information, is said to be very weak in comparison to the EU Directive.<sup>233</sup>

The APEC Cross-Border Privacy Rules (CBPR) System, which has been in place since 2011, is a framework developed by APEC economies to promote privacy regulation interoperability through the enforcement of minimum standards. The CBPR System is not mandatory for APEC economies, and even when they do, businesses may opt out of seeking certification under the System. At the moment, the System is only open to six of the twenty-one APEC economies.<sup>234</sup>

By adhering to the CBPR System, an economy confirms its participation in the Cross-Border Privacy Enforcement Arrangement (CPEA), a regional framework for cooperation on privacy enforcement. Simultaneously, it confirms its intention to use at least one Accountability Agent, which is a third-party oversight entity approved by the Joint Oversight Panel. Adherence does not preclude a member economy from retaining

---

<sup>229</sup> Malcolm Crompton & Peter Ford, *Implementing the APEC Privacy Framework: A New Approach* Iapp.org (2005), <https://iapp.org/news/a/2005-12-implementing-the-apec-privacy-framework-a-new-approach/> (last visited Sep 29, 2021).

<sup>230</sup> *Id.*

<sup>231</sup> APEC Privacy Framework (2015), principle 9. [https://www.apec.org/-/media/APEC/Publications/2017/8/APEC-Privacy-Framework-\(2015\)/217\\_ECSG\\_2015-APEC-Privacy-Framework.pdf](https://www.apec.org/-/media/APEC/Publications/2017/8/APEC-Privacy-Framework-(2015)/217_ECSG_2015-APEC-Privacy-Framework.pdf)

<sup>232</sup> Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (2008), <https://www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/31-cross-border-data-flows/introduction-139/> (last visited Sep 29, 2021).

<sup>233</sup> *Id.*

<sup>234</sup> Francesca Casalinii & Javier López González, *Trade and Cross-Border Data Flows*, OECD Trade Policy Papers (2019), [https://www.oecd-ilibrary.org/trade/trade-and-cross-border-data-flows\\_b2023a47-en](https://www.oecd-ilibrary.org/trade/trade-and-cross-border-data-flows_b2023a47-en) (last visited Sep 29, 2021).

its own privacy regulation; rather, it requires the appointment of a data protection authority (DPA) charged with legally enforcing the privacy policies certified by the Accountability Agent.<sup>235</sup>

Additionally, even if a business is located in an adherent economy, it is not required to comply with the CBPR privacy framework unless the business voluntarily seeks certification under the framework. To accomplish this, the business must create a privacy policy that is consistent with the framework and is subjected to review by a competent Accountability Agent. Once approved, the company's privacy policy is “whitelisted” as compliant with APEC's regional privacy standards. As a result, it assumes responsibility for enforcing applicable privacy laws against both the domestic relevant authority and an Accountability Agent.<sup>236</sup>

Although the CBPR System is intended for data controllers only, a Privacy Recognition for Processors (PRP) has been developed recently to assist processors in gaining the trust of data controllers.<sup>237</sup>

### 5.2.3 EUROPEAN UNION

“The General Data Protection Regulation seeks to harmonize the protection of natural persons' fundamental rights and freedoms in relation to processing activities and to ensure the free flow of personal data between the EU Member States.”<sup>238</sup> The GDPR establishes a clear set of principles<sup>239</sup> and particularly stringent protection standards in the form of enhanced user rights (such as the right to be forgotten,<sup>240</sup> the right to

---

<sup>235</sup> *Id.*

<sup>236</sup> *Id.*

<sup>237</sup> *Id.*

<sup>238</sup> 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) [hereinafter GDPR], at art 3. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>

<sup>239</sup> Article 5 of the GDPR specifies that personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject (principle of lawfulness, fairness and transparency); collected for specified, explicit and legitimate purposes (principle of purpose limitation); processing must also be adequate, relevant and limited to what is necessary (principle of data minimization); as well as accurate and, where necessary, kept up to date (principle of accuracy); data is to be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (principle of storage limitation); data processing must be secure (principle of integrity and confidentiality); and the data controller is to be held responsible (principle of accountability). *Id.*, at art. 5.

<sup>240</sup> *Id.* at art. 17.

transparent information,<sup>241</sup> the right of access to personal data,<sup>242</sup> the right to data portability,<sup>243</sup> the right to object,<sup>244</sup> and the right not to be subject to automated decision-making, including profiling).<sup>245</sup> Consent conditions,<sup>246</sup> which are a necessary condition for lawful data processing,<sup>247</sup> have also been amended to strengthen the user's informational sovereignty. Additionally, the data subject has the right at any time to revoke her consent.<sup>248</sup>

The European Union's (EU) data protection law restricts personal data transfers outside the European Economic Area (EEA).<sup>249</sup> “Following the General Data Protection Regulation's (GDPR) implementation in 2018, the European Union (EU) has been working to maintain high standards of data protection for EU citizens' personal data transfers worldwide. To ensure compliance with these standards, it has two highly effective tools at its disposal. The adequacy decision is the first tool.”<sup>250</sup> The GDPR categorizes countries into two groups when it comes to cross-border data transfers: those that have received an 'adequacy decision' from the European Commission stating that they provide an adequate level of personal data protection (currently 12 countries excluding the EU–US Privacy Shield framework, which was recently declared invalid by the CJEU<sup>251</sup>) and all other countries.<sup>252</sup> Personal data transfers are permitted without restriction only if the destination country, territory, or international organization ensures an “adequate” level of personal data protection.<sup>253</sup> The term “adequate,” as

---

<sup>241</sup> *Id.* at art. 12.

<sup>242</sup> *Id.* at arts. 13–15, 19.

<sup>243</sup> *Id.* at art. 20.

<sup>244</sup> *Id.* at art. 21.

<sup>245</sup> *Id.* at art. 22.

<sup>246</sup> *Id.* at art. 4(11). Article 4(11) of the GDPR clarifies the concept of consent. It states, “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.”

<sup>247</sup> *Id.* at art. 7. There are special conditions applicable to child's consent. The processing of personal data based on consent pursuant to Article 6 (1) is only lawful, if the child is at least 16 years old, or consent is given or authorized by the holder of parental responsibility. Member States can provide by law for a lower age, but not below thirteen. *Id.* at art. 8(1).

<sup>248</sup> See, European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679 Adopted on 4 May 2020.

<sup>249</sup> Svetlana Yakovleva, *Personal Data Transfers in International Trade and EU Law: A Tale of Two 'Necessities'*, 21 THE JOURNAL OF WORLD INVESTMENT & TRADE 881-919 (2020).

<sup>250</sup> David Scholte, EU Data Protection in Trade Agreements KSLR EU Law Blog (2021), <https://blogs.kcl.ac.uk/kslreuropeanlawblog/?p=1524> (last visited Sep 29, 2021).

<sup>251</sup> CJEU, C-311/18, *Data Protection Commissioner v Facebook Ireland Ltd*, Maximillian Schrems, ECLI:EU:C:2020:559 (Schrems II).

<sup>252</sup> GDPR, art 45.

<sup>253</sup> *Id.*

defined by the European Union's Court of Justice (“CJEU”), refers to a level of protection for fundamental rights and freedoms that is “essentially equivalent” to that guaranteed by the E.U. Charter of Fundamental Rights.<sup>254</sup> The European Commission assesses the adequacy of a country, territory, or international organization's data protection regime unilaterally, taking into account its legal and administrative mechanisms for personal data protection.<sup>255</sup> If the Commission makes a favourable determination, it issues a legally binding “adequacy decision.”<sup>256</sup> Transfers of personal data to countries, territories, or international organizations that have not received an adequacy decision are permitted only if the data controller or possessor implements “appropriate safeguards” (such as standard contractual clauses, binding corporate rules, certification, or codes of conduct).<sup>257</sup> Exporters of personal data may rely on limited exemptions in exceptional circumstances (such as the data subject's unambiguous consent or the performance or conclusion of a contract with or in the interest of the data subject).<sup>258</sup> However, the exemptions may be used only for non-repetitive and ad hoc transfers.<sup>259</sup> Under the layered approach, data exporters must first “encourage possibilities to frame the transfer” with one of the adequate safeguards before relying on these derogations.<sup>260</sup>

In short, personal data can be freely transferred outside the EEA to third countries that have been 'cleared' as providing an adequate level of protection. Transfers of personal data to other countries are permitted only if the data controller has implemented adequate safeguards, such as the European Commission-approved SCCs, binding corporate rules (BCRs), approved industry codes of conduct, or certification.<sup>261</sup> SCCs were the most widely used tool for systematic international transfers of personal data to countries without an adequacy decision until recently.<sup>262</sup> Although the CJEU

---

<sup>254</sup> Case C-362/14, Maximilian Schrems v Data Protection Commissioner, 2015 EUR-Lex 62014CJ0362 (Oct. 6, 2015).

<sup>255</sup> For a list of criteria for assessment, See, *Supra* note 34, art. 45(2).

<sup>256</sup> Consolidated Version of the Treaty on the Functioning of the European Union, art. 288, October 26, 2012 O.J. (C 326) 47–390. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN>

<sup>257</sup> GDPR, arts. 46–47.

<sup>258</sup> *Id.* art. 49.

<sup>259</sup> European Data Protection Board, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, Adopted on 25 May 2018, at 4, 8.

[https://edpb.europa.eu/sites/default/files/files/file1/edpb\\_guidelines\\_2\\_2018\\_derogations\\_en.pdf](https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf)

<sup>260</sup> *Id.* at 4.

<sup>261</sup> GDPR, arts 40(2), 42(2), 46.

<sup>262</sup> IAPP–EY Annual Governance Report (2019), showing that 88% of personal data transfers from the EU to the United States are based on the SCCs.

concluded in the 2020 Schrems II decision that SCCs are valid in light of the EU Charter, the Court explained that their use is permitted in practice only if they result in a standard of protection for transferred personal data that is essentially equivalent to that in the EU.<sup>263</sup>

The second tool is data protection provisions in EU-third-country trade agreements. (See CETA art. 28.3(2)(ii), JEFTA art. 8.3, and EU-Singapore FTA art. 8.62(e)(ii).)<sup>264</sup>

Furthermore, the GDPR's territorial scope has been expanded. Article 3(1) defines the territorial scope as personal processing data in the course of a controller's or processor's activities in the EU, regardless of whether the processing takes place within the EU.<sup>265</sup> However, the GDPR applies to a controller or processor not established in the EU if the processing activities are related to (a) the offering of goods or services to such data subjects in the EU, regardless of whether payment of the data subject is required; or (b) the monitoring of their behaviour in the EU.<sup>266</sup> This is a significant expansion of the EU's data protection law's scope and is certain to have a significant impact on its implementation, potentially making it applicable to a large number of the US and other foreign companies targeting the EU market.<sup>267</sup>

“The EEA Agreement covers EU data protection legislation with broad application to commercial activities, such as the General Data Protection Regulation (EU) 2016/679 and all related “adequacy decisions” allowing international transfers of personal data to

---

[http://startupoba.com.br/portaldaprivacidade.com.br/wp-content/uploads/attachments/28563d\\_01043d7b2e454271b15caf16d548a741.pdf](http://startupoba.com.br/portaldaprivacidade.com.br/wp-content/uploads/attachments/28563d_01043d7b2e454271b15caf16d548a741.pdf) (last accessed Sep 29, 2021)

<sup>263</sup> Schrems II (n 4) paras 96, 99, 100, 133–37, 142; Kuner, Christopher. “The Schrems II Judgment of the Court of Justice and the Future of Data Transfer Regulation.” European Law Blog, Europeanlawblog.eu, 17 July. 2020, <https://europeanlawblog.eu/2020/07/17/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-transfer-regulation/>. (last accessed Sep 29, 2021)

<sup>264</sup> *Supra* note 250.

<sup>265</sup> GDPR, at art. 3(1).

<sup>266</sup> *Id.* at art. 3(2); See also, European Data Protection Board, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), 12 November 2019, [https://edpb.europa.eu/sites/default/files/files/file1/edpb\\_guidelines\\_3\\_2018\\_territorial\\_scope\\_after\\_public\\_consultation\\_en\\_1.pdf](https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf)

<sup>267</sup> See, e.g., Paul M. Schwartz, *Information Privacy in the Cloud*, 161 UNIVERSITY OF PENNSYLVANIA LAW REVIEW (2013); OMER TENE & CHRISTOPHER WOLF, OVEREXTENDED: JURISDICTION AND APPLICABLE LAW UNDER THE EU GENERAL DATA PROTECTION REGULATION (2013); Mira Burri & Rahel Schär, *The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy*, 6 JOURNAL OF INFORMATION POLICY 479 (2016); Christopher Kuner, *Reality and Illusion in EU Data Transfer Regulation Post Schrems*, 18 GERMAN LAW JOURNAL 881-918 (2017).

counterparties outside the EEA, as well as the e-Privacy Directive 2002/58/EC and related acts like Regulation (EU) 2016/679. As a result, citizens of the EEA EFTA States - Iceland, Liechtenstein, and Norway - and EU citizens enjoy the same level of protection. Controllers and processors of personal data who are based in an EEA EFTA State are bound by EU legislation, and their compliance is monitored by each EEA EFTA State's independent data protection authority.”<sup>268</sup>

“The European Commission's 2018 endorsement of “EU horizontal provisions on cross-border data flows and protection of personal data and privacy in the Digital Trade Title of EU trade agreements” enables the EU to include measures in trade agreements to facilitate cross-border data flows while fully protecting individuals' fundamental rights to data protection and privacy. The horizontal provisions strike a balance between public and private interests by allowing the EU to address protectionist practices in third countries regarding digital trade while also ensuring that trade agreements cannot be used to undermine the high level of protection guaranteed by the EU Charter of Fundamental Rights and EU data protection legislation.”<sup>269</sup>

According to some, the EU's treatment of services and service providers from countries with and without an adequacy decision may constitute a violation of the MFN principle.<sup>270</sup> Additionally, restrictive rules for transfers to countries that have not received an adequacy decision have been characterized as discrimination against foreign service providers, particularly those without an establishment or business partner in the EEA, and providers from the EEA, and thus constitute another potential

---

<sup>268</sup> Data Protection, European Free Trade Association, Efta.int, <https://www.efta.int/EEA/Data-Protection-505036> (last visited Sep 29, 2021).

<sup>269</sup> EDPS/2021/03, Data protection is non-negotiable in international trade, [https://edps.europa.eu/system/files/2021-02/edps-2021-03-tca\\_uk\\_en.pdf](https://edps.europa.eu/system/files/2021-02/edps-2021-03-tca_uk_en.pdf)

<sup>270</sup> See, eg María Verónica PEREZ ASINARI, Is there any Room for Privacy and Data Protection within the WTO Rules?, 9 ELECTRONIC COMMISSION LAW REVIEW 249-280 (2002); S. Yakovleva & K. Irion, *The Best of Both Worlds? Free Trade in Services and EU Law on Privacy and Data Protection*, 2 EUROPEAN DATA PROTECTION LAW REVIEW 191-208 (2016); Kristina Irion, Svetlana Yakovleva & Marija Bartl, Trade and Privacy: Complicated Bedfellows? How to Achieve Data Protection-Proof Free Trade Agreements, independent study commissioned by BEUC et al, Amsterdam, Institute for Information Law (IViR) (2016); Lucas Bergkamp, *EU Data Protection Policy - The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-Driven Economy*, 18 COMPUTER LAW & SECURITY REVIEW: THE INTERNATIONAL JOURNAL OF TECHNOLOGY LAW AND PRACTICE 31-47 (2002); PERRY KELLER, EUROPEAN AND INTERNATIONAL MEDIA LAW: LIBERAL DEMOCRACY, TRADE, AND THE NEW MEDIA (2011); Carla L. Reyes, *WTO-Compliant Protection of Fundamental Rights: Lessons from the EU Privacy Directive*, 12 MELB. J. INT'L L. 141 (2011); Nivedita Sen, *Understanding the Role of the WTO in International Data Flows: Taking the Liberalization or the Regulatory Autonomy Path?*, 21 JOURNAL OF INTERNATIONAL ECONOMIC LAW 323-348 (2018).

violation of the GATS, namely the obligation to provide national treatment.<sup>271</sup> When it is discovered that a measure violates one or more GATS commitments, it may still be retained for a variety of reasons. In the GDPR context, Articles V<sup>272</sup> and XIV<sup>273</sup> GATS provide two possible defences.<sup>274</sup>

“The EU is a vocal proponent of liberalizing (digital) trade, but it will always fiercely defend its data protection standards; this is stated explicitly in the statement that “EU data protection rules cannot be subject to negotiations in a free trade agreement”.”<sup>275</sup>

#### 5.2.4 UNITED STATES

The United States' data protection laws cover fewer fundamental data protection principles and in a more limited manner than their European Union counterparts.<sup>276</sup>

Although the US has articulated a clear position on data privacy in trade agreements, the US does not have a unified data privacy policy.<sup>277</sup> “The United States has a number of sector and medium-specific national privacy or data security laws, including those governing financial institutions, telecommunications companies, personal health

---

<sup>271</sup> Samuel Coldicutt and Nivedita Sen, Testing the GDPR's WTO readiness Linklaters, <https://www.linklaters.com/en/insights/blogs/tradelinks/testing-the-gdprs-wto-readiness> (last visited Sep 29, 2021); S. Yakovleva & K. Irion, *The Best of Both Worlds? Free Trade in Services and EU Law on Privacy and Data Protection*, 2 EUROPEAN DATA PROTECTION LAW REVIEW 191-208 (2016)

<sup>272</sup> GATS Article V enables WTO Members to enter preferential trade agreements that further liberalise trade and facilitate economic integration in comparison to other WTO Members. This Article may be used to justify entering into an otherwise GATS-incompatible agreement if certain “internal” and “external” conditions are met. The first is a measure of how much an agreement liberalises services trade in terms of sectoral coverage and elimination of discrimination. The second condition, on the other hand, concerns WTO Members who are not parties to the arrangement and requires that they do not face an increase in the “overall level of barriers to trade in services” as a result of it.

<sup>273</sup> GATS Article XIV contains a general exception clause that allows parties to deviate from their GATS obligations in order to comply with domestic laws and regulations, including those aimed at protecting individuals' privacy.

<sup>274</sup> Federica Velli, *The Issue of Data Protection in EU Trade Commitments: Cross-border Data Transfers in GATS and Bilateral Free Trade Agreements*, 4(3) EUROPEAN PAPERS - A JOURNAL ON LAW AND INTEGRATION 881-894 (2019).

<sup>275</sup> COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation COM/2020/264 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0264&from=EN>

<sup>276</sup> Paul M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARVARD LAW REVIEW (2013), at 1976.

<sup>277</sup> Rachel F. Fefer, Congressional Research Service, R45584, *Data Flows, Online Privacy, and Trade Policy*(2020).



information, credit report information, children's information, telemarketing, and direct marketing.”<sup>278</sup>

“Hundreds of privacy and data security laws exist in the United States' 50 states and territories, including requirements for data safeguarding, data disposal, privacy policies, appropriate use of Social Security numbers, and data breach notification. California alone has over 25 state privacy and data security laws, including the recently enacted California Consumer Privacy Act of 2018, which will be significantly amended by the California Consumer Privacy Rights Act, 2023. The CCPA is cross-sectoral in the application and establishes broad definitions and individual rights, as well as significant requirements and restrictions on the collection, use, and disclosure of personal information. Several other states in the United States are currently considering and debating state-level privacy legislation; in some ways, such legislation is similar to the CCPA, but it includes some additional or materially different requirements. As a result, it is highly likely that additional state-level privacy laws will be enacted in the United States that impose requirements that go beyond or differ materially from those of the CCPA.”<sup>279</sup>

While the FTC enforces consumer protection laws and requires consumers to be informed and consent to the use of their data, the FTC lacks the mandate and resources necessary to enforce broad online privacy protections. There is growing support among some members of Congress and the Administration for a more comprehensive US data privacy policy.<sup>280</sup>

“Furthermore, the US Federal Trade Commission (FTC) has authority over a wide range of commercial entities in order to prevent and protect consumers from unfair or deceptive trade practices, including materially unfair privacy and data security practices.”<sup>281</sup>

“The US has proposed or enacted a few data localization requirements, the majority of which pertain to government procurement. Most recently, the US pushed for an

---

<sup>278</sup> Law in United States - DLA Piper Global Data Protection Laws of the World, Dlapiperdataprotection.com (2021), <https://www.dlapiperdataprotection.com/index.html?t=law&c=US&c2=> (last visited Sep 29, 2021).

<sup>279</sup> *Id.*

<sup>280</sup> *Supra* note 277.

<sup>281</sup> *Supra* note 278.

exemption for financial services data from Trans-Pacific Partnership rules prohibiting countries from enacting data flow barriers. However, after the agreement was finalized, the US sought to limit the scope of this provision through bilateral discussions and provisions in the ongoing trade-in services negotiations. In 2016, the Internal Revenue Service issued publication 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies, stating (section 9.3.15.7) that federal agencies must “restrict the location of information systems that receive, process, store, or transmit [federal tax information] to areas within United States territories, embassies, or military installations.” The United States Department of Defense revised its rules in 2015 to require that all cloud computing service providers that work for the department store data domestically. Domestic data storage requirements are occasionally included in other federal public procurement contracts, but they do not constitute an explicit government policy. Similarly, certain state and local governments impose these requirements as part of their contracting processes. Google, for example, was required to store its data in the continental United States as part of its contract with the City of Los Angeles. Tennessee enacted legislation (SB 2344) in 2004 that gives local providers preference when evaluating proposals for state-level procurement contracts requiring data entry or call center services. When the contract is performed by US citizens or other persons authorized to work in the United States, the preference is granted. Similarly, in 2004, an Ohio state representative introduced a bill (No. 459) that would prohibit the transfer of personal data outside the United States without prior written consent in connection with any state procurement project. The bill was never enacted into law. Similar legislation has been proposed in Missouri and several other states. In 2011, a New York State senator introduced legislation (S3713) prohibiting the transfer of personal information outside of the United States without the consumer's prior written consent. It was intended to favour domestic businesses while tangentially linking offshore data storage to consumer fraud and theft.”<sup>282</sup>

The CJEU invalidated two commercial data transfer agreements between the United States and the European Union, most recently the Privacy Shield Framework in July 2020. Since 2016, Privacy Shield has provided a mechanism for EU citizens' personal

---

<sup>282</sup> Nigel Cory, Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost? Itif.org (2021), <https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost> (last visited Sep 29, 2021).

data to be transferred to the US while adhering to EU data protection rules. Privacy Shield sought to address concerns raised in a 2015 CJEU decision invalidating a similar US-EU data transfer agreement from 2000, the Safe Harbor Agreement. Additionally, Privacy Shield was developed in anticipation of the EU's GDPR, which took effect in May 2018 and established new individual rights and data protection requirements throughout the EU. The CJEU, however, found that Privacy Shield did not comply with EU data protection standards due to the breadth of US data collection powers authorized by US electronic surveillance laws and the absence of redress mechanisms for EU citizens. Additionally, the CJEU ruling increased due diligence requirements for data exporters who transfer personal data to the United States via another EU mechanism known as standard contractual clauses (SCCs).<sup>283</sup>

Historically, the United States has sought a balance between trade, privacy, and security. The United States' data flow policy priorities are articulated in the United States Trade Representative's (USTR) Digital 2 Dozen report, which was first developed during the Obama Administration,<sup>284</sup> and the Trump White House's 2017 National Security Strategy.<sup>285</sup> Both administrations emphasize the importance of privacy protection, cross-border data flow, and an interoperable internet. These documents establish the United States' position that the free flow of data is compatible with privacy protection. Recent free trade agreements formalize the United States' position into legally binding international commitments.<sup>286</sup>

## **5.2.5 PEOPLE'S REPUBLIC OF CHINA**

“China's Cybersecurity Law (CSL) establishes the legal framework for data localization and cross-border data transfer requirements.”<sup>287</sup> “China's recently enacted Data Security Law (DSL) establishes specific requirements for the transfer of sensitive data abroad and approval procedures for the provision of data requested by foreign judicial

---

<sup>283</sup> Congressional Research Service, U.S.-EU Privacy Shield (2021), <https://www.everycrsreport.com/reports/IF11613.html>. (last visited Sep 29, 2021).

<sup>284</sup> Ustr.gov, <https://ustr.gov/sites/default/files/Digital-2-Dozen-Updated.pdf> (last visited Sep 29, 2021).

<sup>285</sup> Nationalsecurityforum.org, <https://nationalsecurityforum.org/wp-content/uploads/2018/01/NSS-Final-12-18-2017-0905-2.pdf> (last visited Sep 29, 2021).

<sup>286</sup> *Supra* note 277.

<sup>287</sup> Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017), New America, <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/> (last visited Sep 29, 2021).

and law enforcement authorities.”<sup>288</sup> “Additionally, the second draught of the Personal Information Protection Law (PIPL) contains provisions requiring personal information handlers to adhere to certain standards when transferring personal information overseas.”<sup>289</sup> “Two additional measures on assessing the security of cross-border data transfers were published in 2017 and 2019, respectively, establishing a framework for cross-border data transfers. The Information Security Technology Guidelines for Cross-Border Data Security Assessment supplement the details of the drafted measures and the law, serve as a recommended standard, and provide practical guidance for complying with cross-border data transfers.”<sup>290</sup>

“The CSL became effective on 1 July 2017 and regulates how “critical information infrastructure operators (CIIOs) shall store personal information and critical data gathered and produced during operations within the PRC territory”.”<sup>291</sup> “Where such information and data must be provided to overseas parties for business purposes, a security assessment shall be carried out in accordance with the measures developed by the Cyberspace Administration of China (CAC) in collaboration with the relevant departments of the People's Republic of China's State Council. The law applies only to industries that have critical information infrastructure (CII). The proposed Regulations on the Security Protection of CII expand the definition of CIIs to include entities that provide cloud computing, big data, and other large-scale public information network services.”<sup>292</sup>

“According to the Law, CII operators must store personal information and other important data collected in mainland China within mainland China's borders. Security assessments and approval from industry regulatory bodies are required for industries

---

<sup>288</sup> Translation: Data Security Law of the People's Republic of China, DigiChina, <https://digichina.stanford.edu/news/translation-data-security-law-peoples-republic-china> (last visited Sep 29, 2021).

<sup>289</sup> Translation: Personal Information Protection Law of the People's Republic of China (Effective Nov. 1, 2021), DigiChina, <https://digichina.stanford.edu/news/translation-personal-information-protection-law-peoples-republic-china-effective-nov-1-2021> (last visited Sep 29, 2021).

<sup>290</sup> Cross-Border Data Transfer and Data Localization Requirements in China, ISACA, <https://www.isaca.org/resources/news-and-trends/industry-news/2021/cross-border-data-transfer-and-data-localization-requirements-in-china> (last visited Sep 29, 2021).

<sup>291</sup> *Supra* note 287.

<sup>292</sup> Translation: Critical Information Infrastructure Security Protection Regulations (Effective Sept. 1, 2021), DigiChina, <https://digichina.stanford.edu/news/translation-critical-information-infrastructure-security-protection-regulations-effective-sept> (last visited Sep 29, 2021).

such as banking and specific types of data such as geolocation, making any transfers outside of mainland China nearly impossible.”<sup>293</sup>

“The CAC has published two measures on cross-border data security assessment that are still in draft form and have nonbinding legal effects: the 2019 measures specifically for personal information<sup>294</sup> and the 2017 measures for personal information and important data<sup>295</sup>, and both proposed measures complement the CSL by establishing stringent data localization requirements, proposing mechanisms for security assessment for MNEs, and extending the CSL's applicability beyond CIOs to all network operators, which are broadly defined as the owner or manager of a network or a network service provider. Both measures include a list of critical factors to consider when conducting a security assessment of a cross-border data transfer (i.e., the necessity of the data transfer and the privacy consent of the data subject). There are, however, some distinctions between the two measures. The 2017 measures require cross-border data transfers to be based on “principle-allowed and exception-prohibited” transfers, whereas the 2019 measures require only “approval-based” transfers. In terms of triggering a regulatory assessment, the 2019 measures expand the conditions to cover all cross-border data transfer scenarios, compared to the six limited conditions required by the 2017 measures (i.e., where the data involves personal information of more than 500,000 individuals or the data volume exceeds 1,000GB). According to the 2019 measures, the requirements for the roles of relevant authorities for report review have been changed from industrial administrations, supervisory authorities, or CAC authorities under the 2017 measures to provincial-level cyberspace authorities.”<sup>296</sup>

“The CSL, the newly issued DSL, and the upcoming PIPL all aim to strengthen the rules governing the cross-border provision of personal information and to establish stringent requirements for governing cross-border data security management, including

---

<sup>293</sup> China's Cybersecurity Law: Data Cross-Border Transfer, Protiviti.com, <https://www.protiviti.com/SG-en/insights/pov-data-cross-border-transfer> (last visited Sep 29, 2021).

<sup>294</sup> Translation: New Draft Rules on Cross-Border Transfer of Personal Information Out of China, New America, <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-new-draft-rules-cross-border-transfer-personal-information-out-china/> (last visited Sep 29, 2021).

<sup>295</sup> Notice of the State Internet Information Office on the Public Consultation on the “Measures for the Security Evaluation of the Exit of Personal Information and Important Data (Draft for Solicitation of Comments)”-Office of the Central Committee of the Communist Party of China Cyber Security and Information Technology, Cac.gov.cn, [http://www.cac.gov.cn/2017-04/11/c\\_1120785691.htm](http://www.cac.gov.cn/2017-04/11/c_1120785691.htm) (last visited Sep 29, 2021).

<sup>296</sup> *Supra* note 290.

penalties. The legislative authority will enhance security assessment mechanisms further by expanding the types of security safeguards available, such as self-assessment, regulatory assessment, or approval, and by expanding the scope of application beyond CIIOs to network operators, data handlers, and personal information handlers. The most recent publication of the Financial Data Security Data Lifecycle Security Specification establishes stricter data localization requirements for China's financial industry, which may require significant effort and expense if such data is not currently stored in China.”<sup>297</sup>

PIPL, which was issued on 29 April 2021 in response to public consultations, establishes safeguards for the export of personal information and data localization requirements. There are four significant revisions: Stricter requirements for data localization, Alternative safeguards for the transfer of personal data across borders, Mandatory risk assessment requirements, Requirements for obtaining necessary approvals.<sup>298</sup>

“The DSL, which was published on 10 June 2021 and will take effect on 1 September 2021, establishes some high-level data security principles and restrictions. Although the DSL established requirements for export control over data relating to controlled items necessary for the fulfilment of international obligations and the maintenance of national security, it does not specify the types of data subject to export control. The DSL's requirements for cross-border data transfer of critical data are based on the CSL but with three significant changes: Separate requirements for international transfers, relevant approval rules have been updated and specified punishment for violations.”<sup>299</sup>

“China has a highly regulated legal system based on the principle of “principle prohibited and exception allowed” in light of regulatory requirements for data localization and cross-border data transfer. Personal financial information collected within the PRC's territory shall be stored, processed, and analyzed primarily in China, subject to statutory exceptions.”<sup>300</sup> “The Financial Data Security Data Lifecycle

---

<sup>297</sup> *Id.*

<sup>298</sup> *Id.*

<sup>299</sup> *Id.*

<sup>300</sup> Notice of the People's Bank of China on Printing and Distributing the “Implementation Measures for the Protection of the Rights and Interests of Financial Consumers of the People's Bank of

Security Specification, which took effect on 8 April 2021,<sup>301</sup> specifies that level 5 data (critical data that is primarily used in large financial institutions for critical business such as financial transactions that could jeopardize national security or the rights and interests of the public if security is breached) generated in China must be stored exclusively in China. Although financial data at levels 1 to 4 must be stored primarily in China, the Chinese regulatory requirements allow for overseas access and transfer of personal information with the necessary compliance safeguards in place, such as consent and security assessment provided by financial institutions.”<sup>302</sup>

## 5.2.6 INDIA

India's draft Personal Data Protection Bill would impose broad data localization requirements and restrict the cross-border transfer of certain data.<sup>303</sup> In contrast to the European Union, India does not specify mechanisms for cross-border data flows. Officials in the United States have expressed concern about India's localization requirements.<sup>304</sup>

“India has proposed and enacted a number of laws and regulations requiring the localization of data. As part of a 2011 privacy rule change, India's Ministry of Communications and Technology enacted data transfer requirements that could be used to restrict data flows containing personal information (but has not been). These rules restrict the transfer of “sensitive personal data or information” to two narrow circumstances: when the transfer is “necessary” or when the subject consents to the transfer. Because establishing that a data transfer is “necessary” is difficult, this provision effectively prohibits transfers abroad except with an individual's consent. The

---

China”\_State Council Communiqué No. 21 of 2017\_Chinese Government Website, Gov.cn, [http://www.gov.cn/gongbao/content/2017/content\\_5213211.htm](http://www.gov.cn/gongbao/content/2017/content_5213211.htm) (last visited Sep 29, 2021).

<sup>301</sup> People’s Bank of China (PBOC), Financial Data Security Data Lifecycle Security Specification, China, Hankunlaw.com, <https://www.hankunlaw.com/downloadfile/newsAndInsights/c4b38d77b09fc65076a94458637c0e35.pdf> (last visited Sep 29, 2021).

<sup>302</sup> *Supra* note 290.

<sup>303</sup> Ashi Bhat and Suneeth Katarki, The Debate – Data Localization and Its Efficacy - Privacy - India, Mondaq.com (2018), <https://www.mondaq.com/india/privacy-protection/736934/the-debate-data-localization-and-its-efficacy> (last visited Sep 29, 2021).

<sup>304</sup> U.S. Trade Representative, 2018 National Trade Estimate Report on Foreign Trade Barriers, 2018. [https://ustr.gov/sites/default/files/files/Press/Reports/2018%20National%20Trade%20Estimate%20Report.pdf?utm\\_source=POLITICO.EU&utm\\_campaign=f17a177eee-EMAIL\\_CAMPAIGN\\_2018\\_04\\_02&utm\\_medium=email&utm\\_term=0\\_10959edeb5-f17a177eee-189017913](https://ustr.gov/sites/default/files/files/Press/Reports/2018%20National%20Trade%20Estimate%20Report.pdf?utm_source=POLITICO.EU&utm_campaign=f17a177eee-EMAIL_CAMPAIGN_2018_04_02&utm_medium=email&utm_term=0_10959edeb5-f17a177eee-189017913).

ministry clarified that these rules apply only to businesses that collect data on Indians and only if the business is headquartered in India. While these laws appear to be restrictive on the surface, India has thus far refrained from enforcing the law's requirement of local data storage. In 2012, India enacted a “National Policy on Data Sharing and Accessibility,” requiring that government data (data owned by government agencies or collected with public funds) be stored in local data centers. The Indian National Security Council proposed a policy in February 2014 requiring all email providers to establish local servers for their India operations and requiring that all data associated with communication between two Indian users remain within the country. India enacted the Companies (Accounts) Rules law in 2014, requiring backups of financial information to be stored in India if it is primarily stored overseas.”<sup>305</sup>

### **5.2.7 GENERAL AGREEMENT ON TRADE IN SERVICES**

Individual privacy is protected under the General Agreement on Trade in Services. The GATS is a recognized leader in the field of electronic commerce. It contains the rules of the World Trade Organization (WTO) that regulate data flows.<sup>306</sup>

Within the General Exceptions, as defined in Article XIV, governments are required to take measures to safeguard individuals' privacy when processing and disclosing personal data. The provisions make reference to privacy, morals, public order, health, and fraud prevention as reasons to control data flows.<sup>307</sup>

The GATS contains the data flow principle or, at the very least, its fundamental commercial objective. Capital can be compared to data flows, according to Tuthill. Capital movement across borders is mentioned in a footnote to Article XVI, which deals with market access.<sup>308</sup>

## **5.3 ANALYSIS**

---

<sup>305</sup> *Supra* note 282.

<sup>306</sup> See, Aaditya Mattoo & Joshua P Meltzer, *International Data Flows and Privacy: The Conflict and Its Resolution*, 21 JOURNAL OF INTERNATIONAL ECONOMIC LAW 769-789 (2018).

<sup>307</sup> Tuthill, *supra* note 206.

<sup>308</sup> *Id.*



Without an international treaty to which the EU, the United States, and China would all be parties, they each regulate data exchanges according to their own requirements and philosophies. The United States approach is the simplest, as there are no special requirements for personal data transfers from the United States to a third country. The US is also a vocal opponent of data localization restrictions, which are viewed as trade barriers.<sup>309</sup> EU law is more restrictive but does not include a requirement for data localization, which would require certain personal information to remain within Europe. However, cross-border data transfers are permitted only in accordance with the GDPR's protection standards, that is, to third countries with a data protection level recognized by the European Commission as equivalent to that of the EU, or with the use of appropriate safeguards such as standard contractual clauses or binding corporate rules.<sup>310</sup> Legal scholars have labelled the difference with the United States as a “dramatic distinction.”<sup>311</sup>

While the EU and US models are well-established, they are antagonistic. Both sides of the Atlantic have a distinct philosophy that informs their approach, resulting in divergent legal instruments and levels of protection for individuals. In the European Union, both the right to privacy and the right to data protection are considered fundamental rights and are protected by a comprehensive legal standard. The law has a broad application; it covers all organizations that collect and process personal data. Personal data is a broad term that encompasses all information about an individual. The law provides strong protections for those individuals, which were recently reinforced by the General Data Protection Regulation (“GDPR”)<sup>312</sup>, confirming the EU's direction. In contrast, the United States lacks a comprehensive federal law governing all aspects of data privacy. Rather than that, pertinent provisions are scattered throughout numerous laws regulating a variety of topics and sectors with varying scopes. They may pertain to government agencies, children's data, health data, a focus on data breaches, or be a federal or state law. They typically impose fewer requirements and provide less protection than the EU does. The EU model has demonstrated an increasing influence

---

<sup>309</sup> John Selby, *Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both?*, 25 INTERNATIONAL JOURNAL OF LAW AND INFORMATION TECHNOLOGY 213-232 (2017).

<sup>310</sup> GDPR, art. 46.

<sup>311</sup> Schwartz, *supra* note 276.

<sup>312</sup> GDPR.

on the laws of third countries<sup>313</sup>, at the expense of the US model, which has not achieved the same level of success.<sup>314</sup>

A requirement to store personal information within a country, such as in China, does not exist in either US or EU law but does exist in other countries such as Russia.<sup>315</sup> Provisions governing data localization and restrictions on cross-border transfers of personal data are among the most contentious legal elements, with the least convergence between the three approaches.<sup>316</sup>

The OECD Privacy Guidelines are a soft law instrument, and their fundamental principles are widely recognized as the minimum international standards for data protection.<sup>317</sup> On the other hand, Convention 108 contains stricter provisions than the OECD Privacy Guidelines and is the only internationally legally binding instrument in the field, which means that countries that sign the convention must enact legislation reflecting its principles.<sup>318</sup>

There is growing recognition that countries' data protection laws should begin to converge.<sup>319</sup> There appears to be a push to make the GDPR more of a global baseline for what may become the basic standard in the future. Brazil, India, Japan, and the Republic of Korea have already implemented GDPR-style rules, and the EU is actively promoting their adoption.<sup>320</sup> Additionally, several global digital platforms have begun

---

<sup>313</sup> G. Greenleaf, *The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108*, in *INTERNATIONAL DATA PRIVACY LAW* 68–92 (2012).

<sup>314</sup> See generally, Ryan Moshell, *And Then There Was One: The Outlook for a Self-Regulatory United States Amidst a Global Trend Towards Comprehensive Data Protection Framework*, 37 *TEXAS TECH LAW REVIEW* 357 (2005).

<sup>315</sup> See generally, W. Gregory Voss, *Cross-Border Data Flows, the GDPR, and Data Governance*, 29 *WASH. INT'L. L.J.* 485 (2020); and Federal Law No. 242-FZ of July 21, 2014 on Amending Some Legislative Acts of the Russian Federation in as Much as It Concerns Updating the Procedure for Personal Data Processing in Information-Telecommunication Networks (with Amendments and Additions). <https://pd.rkn.gov.ru/authority/p146/p191/> (last visited Sep 29, 2021)

<sup>316</sup> Emmanuel Pernot-Leplay, *China's Approach on Data Privacy Law: A Third Way Between the U.S. and the EU?*, 8 *PENN STATE JOURNAL OF LAW & INTERNATIONAL AFFAIRS* (2020).

<sup>317</sup> Greenleaf, *supra* note 313, at 73.

<sup>318</sup> Graham Greenleaf, *Convention 108+ and the Data Protection Framework of the EU (Speaking Notes for Conference Presentation)*, *Convention 108+ Tomorrow's Common Ground for Protection?* (Council of Europe, Strasbourg, 21 June 2018). UNSW Law Research Paper No. 18-39 (2018).

<sup>319</sup> Dixon H., "Regulate to Liberate: Can Europe Save the Internet?" *Foreign Affairs* 97(5): 28–32, (2018).

<sup>320</sup> See, Adam Satariano, *G.D.P.R., a New Privacy Law, Makes Europe World's Leading Tech Watchdog* (Published 2018) *Nytimes.com* (2018), <https://www.nytimes.com/2018/05/24/technology/europe-gdpr-privacy.html> (last visited Sep 29, 2021); and Vindu Goel, *India Pushes Back Against Tech 'Colonization' by Internet Giants* (Published 2018)

to standardize their practices globally. Microsoft, for example, has stated that it will adhere to GDPR rules as a global standard, while Apple and Facebook have both called for privacy protections akin to those found in the EU.<sup>321</sup>

The European Union's restrictions on cross-border transfers of personal data undoubtedly limit international trade.<sup>322</sup> The EU data protection framework, which requires a higher level of data protection complemented by restrictions on cross-border transfers of personal data, is mentioned as restricting international digital trade in several sectors in a taxonomy of trade restricting measures prepared by the United States International Trade Commission (“USITC”).<sup>323</sup> The USITC and ECIPE emphasize that cross-border transfer restrictions, in addition to substantive rules restricting the use of personal data and data localization measures, raise the costs of doing business for multinational corporations.<sup>324</sup> More specifically, ECIPE researchers contend that restrictions on cross-border data flows reduce (or, in other words, limit) imports of data-intensive services.<sup>325</sup>

While the US and the EU frame their discourses on digital trade similarly, they clearly disagree on the appropriate balance to strike between the economic benefits of digital trade and societal values such as the protection of privacy and personal data.<sup>326</sup> Even if

---

Nytimes.com (2018), <https://www.nytimes.com/2018/08/31/technology/india-technology-american-giants.html> (last visited Sep 29, 2021).

<sup>321</sup> See, Liam Tung, Microsoft: We're giving you all Euro-style GDPR rights over how we use your data, ZDNet ZDNet (2018), <https://www.zdnet.com/article/microsoft-were-giving-you-all-euro-style-gdpr-rights-over-how-we-use-your-data/> (last visited Sep 29, 2021); and Mehreen Khan & Tim Bradshaw, Apple and Facebook call for EU-style privacy laws in US Ft.com (2018), <https://www.ft.com/content/0ca8466c-d768-11e8-ab8e-6be0dcf18713> (last visited Sep 29, 2021).

<sup>322</sup> Svetlana Yakovleva, *Privacy Protection(ism): The Latest Wave of Trade Constraints on Regulatory Autonomy*, 74 U. MIAMI L. REV. 416 (2020).

<sup>323</sup> David Coffin & et al, United States International Trade Commission, *Global Digital Trade I: Market Opportunities and Key Foreign Trade Restrictions* (2017),

<https://www.usitc.gov/publications/332/pub4716.pdf> (last visited Sep 29, 2021). (“According to input from industry representatives, regulatory and policy measures focused on data protection and privacy affect all kinds of industries. These measures can inhibit global digital trade by U.S. firms due to the increased administrative costs associated with complying with stricter privacy measures that differ from U.S. standards.”).

<sup>324</sup> Id; Martina F. Ferracane, Janez Kren, Erik van der Marel, *The Cost of Data Protectionism*, ECIPE (2018), <https://ecipe.org/blog/the-cost-of-data-protectionism/> (last visited Sep 29, 2021).

<sup>325</sup> See, Martina Ferracane & Erik van der Marel, *Do Data Policy Restrictions Inhibit Trade in Services?*, SSRN Electronic Journal (2019). (showing that “more restrictive data policies, in particular with respect to the cross-border movement of data, result in lower imports in data-intense services for countries imposing them.”).

<sup>326</sup> Susan Aaronson, *Why Trade Agreements are not Setting Information Free: The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights, and National Security*, 14 WORLD TRADE REVIEW 671-700 (2015), at 687, (“Unfortunately, despite their collaboration, the

privacy and personal data protection can be priced, the “optimal” level of protection determined from a legal (fundamental right) approach to privacy and data protection will be lower because the economic calculus does not account for the intrinsic value of privacy and data protection as a fundamental right.<sup>327</sup> A data protection policy that considers both economic and non-economic factors is arguably more likely to ensure a higher level of personal data protection than one that considers only economic efficiency factors.<sup>328</sup>

Countries need more regulatory space to design domestic data protection regimes unless approaches to data protection and privacy are harmonized, which is not feasible due to differences and lack of (political) basis (plus risks of becoming the lowest common denominator). Because other countries' data protection standards are low (perhaps strategically low), countries with higher standards must restrict data transfers.<sup>329</sup> A more extensive form of global governance would be required to achieve deep harmonization of domestic privacy and data protection standards.<sup>330</sup>

International agreements should prioritize the establishment of a legal framework governing the exchange of personal data. The international community should promote digital commerce by not restricting personal data flows but rather by establishing a legal framework that legalizes and protects the market.<sup>331</sup>

Individuals will always have access to privacy frameworks as a means of protection. The distinction is that the individual will retain the right to keep his or her information

---

US and the EU do not completely agree on digital rights . . . . In addition, the US and the EU disagree on the role of the state and business in protecting privacy.”).

<sup>327</sup> Yakovleva, *supra* note 322.

<sup>328</sup> See, e.g., A. Acquisti, L. Brandimarte & G. Loewenstein, *Privacy and Human Behavior in the Age of Information*, 347 *SCIENCE* 509-514 (2015) at 509, (showing that providing users with explicit control mechanisms over their personal data may lead to sharing more sensitive data by users).

<sup>329</sup> On the prospects of harmonizing data protection regimes, see, e.g., H. Jeff Smith, Sandra J. Milberg & Sandra J. Burke, *Information Privacy: Measuring Individuals' Concerns about Organizational Practices*, 20 *MIS QUARTERLY* 167 (1996), at 53 (“What will or will not meet ‘societal expectations’ is highly contingent on a society itself . . . . Thus, a universal regulatory approach to information privacy seems unlikely and would ignore cultural and societal differences.”); see also, Christopher Kuner, *Regulation of Transborder Data Flows Under Data Protection and Privacy Law: Past, Present, and Future*, OECD Digital Economy Papers, No. 187, (2011); Perry Keller, *European and International Media Law: Liberal Democracy, Trade, and the New Media* (2011). But see, Aaditya Mattoo & Joshua P Meltzer, *International Data Flows and Privacy: The Conflict and Its Resolution*, 21 *JOURNAL OF INTERNATIONAL ECONOMIC LAW* 769-789 (2018) (arguing that a common privacy framework could be based on the OECD and APEC data protection frameworks).

<sup>330</sup> Yakovleva, *supra* note 322.

<sup>331</sup> Tlacuilo Fuentes, Itzayana, *Legal Recognition of the Digital Trade in Personal Data*, *MEXICAN LAW REVIEW*, [S.l.], p. 87-117, dec. 2019.

private. In this instance, the doctrine of *volenti non fit injuria* applies. The law restricts protection to the extent that corresponds to the will of those entitled to it. Consent enables lawful conduct in the realm of personal data that would be illegal otherwise.<sup>332</sup>

---

<sup>332</sup> See, Radim Polčák & Dan Jerker B Svantesson, *Private information sovereignty, Information Sovereignty: Data Privacy, Sovereign Powers and the Rule of Law* 81–112 (2017).

## CHAPTER VI:

### CONCLUSIONS AND SUGGESTIONS

The world of big data continues to spin, generating new opportunities, novel approaches to business growth and development, and a slew of novel ways to manage the population's rapidly expanding data mass. As with any significant emerging shift, big data has introduced a number of complications. Internet users are becoming aware of the extent of data misuse and the fact that their data is owned and controlled by others, and they feel helpless as laws across the world address this issue slowly.

At the moment, no agreement exists regarding the law governing intellectual property rights in data. To be patentable, data must first satisfy the requirements of a physical invention or a technological solution to a problem. By virtue of its non-relational nature, an extensive data database cannot be protected by copyright or EU sui generis database protection. A breach of data privacy may jeopardize an organization's ability to protect information as a trade secret.

Determining right-holdership is not always straightforward, as multiple stakeholders frequently contribute to data collection and processing directly or indirectly. A complicated system of exceptions and limitations would need to be implemented, taking other subjects' interests into account. There is a significant disconnect between human creators and their digital tools because the vast majority of work is performed by computer software.

According to the law, ownership is the most comprehensive right that a person can have over an object. Additionally, objects are tangible physical entities that humans can manipulate. As a result, this concept is meaningless when applied to data.

The term “data ownership” raises significant issues and may be inappropriate, as data is not comparable to property or other tangible goods that can be owned or exchanged. Instead, the discussion should center on the rights and controls that individuals, groups, and organizations have over data, taking into account both societal and individual perspectives.

Ownership of data is not synonymous with traditional ownership. It is all about consent and control. Consent is frequently invoked as a mechanism for authorizing the surrender of privacy in the majority of policy proposals advocating for data ownership or privacy as property. All data ownership proposals seek to empower individuals with greater control over their personal information by allowing them to determine when and how much they wish to be compensated for it. As it turns out, this is all about trading, not owning.

Individuals have control over their data under data consent laws, which limit its use and dissemination while allowing businesses to use the exact data for commercial and consumer benefit. While individuals have the ability to restrict the use of their personal data, these limitations demonstrate “control” but not ownership.

On the one hand, privacy protection and information self-determination are inextricably linked to freedom of thought, communication, science, economic competition, and technological innovation, on the other. To protect both types of interests, data is not protected by a proprietary right.

Rather than the concept of “ownership,” the existing legal framework protects de facto “possession.” Due to the lack of a comprehensive property regime that applies to all data, raw data is primarily controlled through contractual and access restriction mechanisms based on factual exclusivity rather than traditional private law ownership.

If a data property right is granted, control will almost certainly erode. When a consumer sells a piece of property, they give up ownership and control of it. Establishing a data property right may also have a detrimental effect on individuals with limited financial resources. It carries the risk of exacerbating inequity. Data ownership can create significant competition risks and is notoriously difficult to regulate. Giving exclusive data ownership rights to specific stakeholder groups may not be the best course of action. Co-ownership of data can create roadblocks and exacerbate inefficiencies caused by the underuse of data.

The establishment of a new right would require extensive planning in advance. Additionally, it would entail taking into account user rights as well as the general public's interest in data access and use. In comparison to physical property ownership

rights, which are binary in nature, data ownership rights are layered, making their determination more difficult.

Creating new ad hoc laws or exclusive rights for data may actually have a negative impact on the free flow of data, outweighing the benefits of establishing this type of ownership right.

The data subject is frequently asserted to be the owner of their data. Simply because a piece of data is associated with a specific individual does not mean that the individual legally “owns” their personal data. The concept of exclusivity complicates the definition of data or information as “property” because it is self-evident that a person can possess data or information that is also known to others without depriving them of it. Indeed, there has historically been a legal reluctance to view ideas, knowledge, information, or data as “property” in the strictest sense.

There is no distinction in current data protection laws between those who have and those who do not have personal data. This means that any recognition of a new intellectual property right, such as the right to data ownership, would require compelling evidence. At the moment, this type of justification does not exist.

After establishing that no one owns the underlying data, it is reasonable to conclude that an urgent need exists for a new normative framework founded on the ethical principle of custodianship to ensure accountability and responsible data sharing among all stakeholders.

Cross-border data flows, and data protection are critical components of economic and trade policy in the digital age. Cross-border data flows have become an integral part of international commerce and the foundation for a variety of digital service models. International trade will invariably be impacted by regulations governing cross-border data flows to protect personal information.

Globalization of digital data and services commerce has not resulted in true convergence or harmonization of data protection and privacy legislation. Globally, nation-states and regions have failed to harmonize data privacy law, opting instead for divergent regulatory models with strategic ramifications. Certain states have enacted legislation affecting international commerce and data flows beyond their borders, while



others regulate data flows through the imposition of data localization requirements. While these complexities have stymied some data flows, international treaties have been used to ensure the free flow of personal data in the future, subject to certain safeguards for data subjects and their data.

The absence of privacy and data protection legislation and divergent approaches among countries that do have such legislation jeopardize fundamental rights, adequate cross-border data flows, and the free flow of information.

There has been a proliferation of “data protection” laws over the last decade or so. Complicating matters further is an organization's requirement to comply with multiple laws when conducting transborder processing. Several of these statutes impose additional security requirements on regulated entities. Regulating bodies are required to conduct inspections and audits on a regular basis to ensure compliance. Another area of concern for the regulating entity is the monitoring and surveillance of transborder data flows.

Both the free flow of information across borders and data subjects' rights must be safeguarded. Trade agreements will almost certainly determine the future of internet governance, including online privacy. As a result, globally binding standards to ensure adequate privacy and data protection safeguards are required. Domestic and international law must work in tandem to regulate cross-border data flows, with international law imposing obligations on domestic law.

It is necessary to establish a comprehensive set of operating rules universally accepted, balanced in its fundamental principles, and practical application. It should ensure that data flows freely across borders. Non-personal data should be included in such harmonizing legislation as well as non-personal data has an economic value that could be leveraged for financial benefit by the creators.

Currently, the European Union has the strictest, and thus best, data protection standards in place. Developing an international legal system would be an excellent place to start by developing a global data protection law based on fundamental principles similar to those found in the EU.

Additionally, the APEC Cross-Border Privacy Framework demonstrates promise in terms of harmonizing cross-border transfers between the EU and Asia-Pacific and establishing a potential global framework for balancing privacy protection and the free flow of information necessary for economic growth.

There should be a clear definition of what constitutes an individual's exclusive right to personal data, as even anonymized data can reveal personally identifiable information when linked together.

The level of control that users have over their data should be increased. Prior informed consent must be obtained at the time of data collection. This should become the standard method rather than the information-only method. He should be informed of the type of data for which access is being requested. He should be informed of how data will be used and with whom it will be shared. When sharing data with a third party, the data principal should be notified and consent to the sharing obtained. Finally, data principals will be aware of which data is being requested and will be willing to allow or deny each request.

Create a transparent and widely accepted market-based system for classifying data and compensating users for data trading. Compensation may take the form of customized services or monetary compensation, and specific data may be completely untradeable.

Blockchain technologies enable a new innovative approach by creating a decentralized user database with anonymity. The data controllers could make use of this.

Individuals should have complete control over their data. He should have the ability to edit data, withdraw consent, and delete data, among other things. There should be a time limit on how long businesses can store data in specific circumstances, such as purchase-related data, because businesses are required by law to keep their personal information for accounting and legal purposes. Following that, it should be deleted regardless of whether the data principal has requested deletion.

Notification of data breaches should be strictly enforced. Following a data breach, the data principal should be informed of the breach, the amount of data compromised, and so on.

The data controller should be held liable for data loss. Stricter sanctions should be enacted. There should be increased enforcement of data use and privacy laws at the national, international, and local levels. All organizations that handle data should be required to have a data protection officer.

## BIBLIOGRAPHY

### BOOKS

1. K KOUL & V. K AHUJA, THE LAW OF INTELLECTUAL PROPERTY RIGHTS (2001)
2. BILL FRANKS, TAMING THE BIG DATA TIDAL WAVE (2012)
3. CAROL L STIMMEL, BIG DATA ANALYTICS STRATEGIES FOR THE SMART GRID (2014)
4. ESTELLE DERCLAYE, THE LEGAL PROTECTION OF DATABASES - A COMPARATIVE ANALYSIS (2008)
5. HENRY CAMPBELL BLACK, OWNERSHIP BLACK'S LAW DICTIONARY (10 ed. 2009)
6. NADEZHDA PURTOVA, PROPERTY RIGHTS IN PERSONAL DATA: A EUROPEAN PERSPECTIVE (2011)
7. OMER TENE & CHRISTOPHER WOLF, OVEREXTENDED: JURISDICTION AND APPLICABLE LAW UNDER THE EU GENERAL DATA PROTECTION REGULATION (2013)
8. PAUL C. ZIKOPOULOS ET AL., UNDERSTANDING BIG DATA: ANALYTICS FOR ENTERPRISE CLASS HADOOP AND STREAMING DATA (2012)
9. PERRY KELLER, EUROPEAN AND INTERNATIONAL MEDIA LAW: LIBERAL DEMOCRACY, TRADE, AND THE NEW MEDIA (2011)
10. ROBIN ELIZABETH HERR, IS THE SUI GENERIS RIGHT A FAILED EXPERIMENT (2008)
11. THOMAS ERL, WAJID KHATTAK & PAUL BUHLER, BIG DATA FUNDAMENTALS: CONCEPTS, DRIVERS & TECHNIQUES (2016)
12. THOMAS ERL, ZAIGHAM MAHMOOD & RICHARDO PUTTINI, CLOUD COMPUTING: CONCEPTS, TECHNOLOGY & ARCHITECTURE, PRENTICE HALL SERVICE TECHNOLOGY SERIES FROM THOMAS ERL. (2013)
13. U.S. COPYRIGHT OFFICE, COMPENDIUM OF U.S. COPYRIGHT OFFICE PRACTICES § 101 (3d ed. 2021)
14. VIKTOR MAYER-SCHONBERGER AND KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK, (Houghton Mifflin Harcourt, 2013)

### WORKS IN COLLECTION

1. Amy Shi-Nash & David R. Hardoon, *Data Analytics and Predictive Analytics in the Era of Big Data*, in INTERNET OF THINGS AND DATA ANALYTICS HANDBOOK 329-345 (Hwaiyu Geng 1 ed. 2016)
2. Estelle Derclaye, *The Database Directive*, in EU COPYRIGHT LAW - A COMMENTARY 298–354 (Irina A. Stamatoudi & Paul Torremans 2014)

3. Francesco Banterle, *Data Ownership in the Data Economy: A European Dilemma*, in EU INTERNET LAW IN THE DIGITAL ERA (Tatiana-Eleni Synodinou et al. 2020)
4. G. Greenleaf, *The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108*, in INTERNATIONAL DATA PRIVACY LAW 68–92 (2012)
5. Herbert Zech, *Data as a Tradeable Commodity*, in EUROPEAN CONTRACT LAW AND THE DIGITAL SINGLE MARKET: THE IMPLICATIONS OF THE DIGITAL REVOLUTION 51-80 (Alberto De Franceschi 2016)
6. Jiannong Cao et al., *Programming Platforms for Big Data Analysis*, in HANDBOOK OF BIG DATA TECHNOLOGIES 65-99 (Albert Y. Zomaya & Sherif Sakr 1 ed. 2017)
7. Julie E. Cohen & William M. Martin, *Intellectual Property Rights in Data*, in INFORMATION SYSTEMS AND THE ENVIRONMENT 45-55 (Deanna J. Richards, Braden R. Allenby & W. Dale Compton 2001)
8. L. Lee Tuthill, *Cross-Border Data Flows: What Role for Trade Rules?*, in RESEARCH HANDBOOK ON TRADE IN SERVICES 357–382 (Pierre Sauvé & Martin Roy 1 ed. 2016).
9. Lisa M. Austin, *The Public Nature of Private Property*, in PROPERTY THEORY: LEGAL AND POLITICAL PERSPECTIVES (James Penner & Michael Otsuka 2018)
10. Michael R. Overly, *Overview of Information Security and Compliance: Seeing the Forest for the Trees*, in BIG DATA (James R. Kalyvas & Michael R. Overly 1 ed. 2014)
11. Solon Barocas & Helen Nissenbaum, *Big Data's End Run around Anonymity and Consent*, in PRIVACY, BIG DATA, AND THE PUBLIC GOOD 44-75 (Julia Lane et al. 2014)

## ARTICLES

1. Acquisti, L. Brandimarte & G. Loewenstein, *Privacy and Human Behavior in the Age of Information*, 347 SCIENCE 509-514 (2015)
2. Aaditya Mattoo & Joshua P Meltzer, *International Data Flows and Privacy: The Conflict and Its Resolution*, 21 JOURNAL OF INTERNATIONAL ECONOMIC LAW 769-789 (2018)
3. Abou Zakaria Faroukhi et al., *Big Data Monetization Throughout Big Data Value Chain: A Comprehensive Review*, 7 JOURNAL OF BIG DATA (2020)
4. Abu Bakar Munir, Siti Hajar Mohd Yasin & Firdaus Muhammad-Sukki, *Big Data: Big Challenges to Privacy and Data Protection*, 9 WORLD ACADEMY OF SCIENCE, ENGINEERING AND TECHNOLOGY INTERNATIONAL

- JOURNAL OF COMPUTER AND INFORMATION ENGINEERING 355-363  
(2015)
5. Addi Ait-Mlouk, Tarik Agouti & Fatima Gharnati, *Mining and Prioritization of Association Rules for Big Data: Multi-Criteria Decision Analysis Approach*, 4 JOURNAL OF BIG DATA (2017)
  6. Alberto De Franceschi & Michael Lehmann, *Data as Tradeable Commodity and New Measures for their Protection*, 1 THE ITALIAN LAW JOURNAL 51-72 (2015)
  7. Amir Khoury, *Intellectual Property Rights for Hubots: On the Legal Implications of Human-like Robots as Innovators and Creators*, 35 CARDOZO ARTS & ENT. LJ 635-665 (2016)
  8. Andreas Boerding et al., *Data Ownership—A Property Rights Approach from a European Perspective*, 11 JOURNAL OF CIVIL LAW STUDIES (2018),
  9. Andrei Shleifer, *State versus Private Ownership*, 12 JOURNAL OF ECONOMIC PERSPECTIVES 133-150 (1998)
  10. Kuner et al., *The Challenge of 'Big Data' for Data Protection*, 2 INTERNATIONAL DATA PRIVACY LAW 47-49 (2012)
  11. Carla L. Reyes, *WTO-Compliant Protection of Fundamental Rights: Lessons from the EU Privacy Directive*, 12 MELB. J. INT'L L. 141 (2011)
  12. Catherine Colston, *Sui Generis Database Right: Ripe for Review?*, 3 JOURNAL OF INFORMATION LAW & TECHNOLOGY (2001)
  13. Christopher Kuner, *Reality and Illusion in EU Data Transfer Regulation Post Schrems*, 18 GERMAN LAW JOURNAL 881-918 (2017)
  14. Daniel Gervais, *Exploring the Interfaces Between Big Data and Intellectual Property Law*, 10 JOURNAL OF INTELLECTUAL PROPERTY, INFORMATION TECHNOLOGY AND E-COMMERCE LAW (2019)
  15. Daniel Gervais, *The Protection Under International Copyright Law of Works Created with or by Computers*, 5 IIC INT'L REV. IND'L PROP. AND COPYRIGHT LAW, 629, 644-45 (1991)
  16. Davide Borelli, *International Trading of Big Data*, 3 ATHENS JOURNAL OF LAW 21-30 (2016)
  17. Dennis Hart, *Ownership as an Issue in Data and Information Sharing: A Philosophically Based Review*, 10 AUSTRALASIAN JOURNAL OF INFORMATION SYSTEMS (2002)

18. Emmanuel Pernet-Leplay, *China's Approach on Data Privacy Law: A Third Way Between the U.S. and the EU?*, 8 PENN STATE JOURNAL OF LAW & INTERNATIONAL AFFAIRS (2020)
19. Federica Velli, *The Issue of Data Protection in EU Trade Commitments: Cross-border Data Transfers in GATS and Bilateral Free Trade Agreements*, 4(3) EUROPEAN PAPERS - A JOURNAL ON LAW AND INTEGRATION 881–894 (2019)
20. Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARVARD LAW REVIEW 1089 (1972)
21. H. Jeff Smith, Sandra J. Milberg & Sandra J. Burke, *Information Privacy: Measuring Individuals' Concerns about Organizational Practices*, 20 MIS QUARTERLY 167 (1996)
22. I.A.T. Hashem et al., *The Role of Big Data in Smart City*, 36 INTERNATIONAL JOURNAL OF INFORMATION MANAGEMENT 748–758 (2016)
23. Ibrar Yaqoob et al., *Big data: From Beginning To Future*, 36 INTERNATIONAL JOURNAL OF INFORMATION MANAGEMENT 1231-1247 (2016)
24. Ignacio Cofone, *Beyond Data Ownership*, 43 CARDOZO LAW REVIEW
25. J.E. Penner, *The "Bundle of Rights" Picture of Property*, 43 UCLA LAW REVIEW 711-820 (1996)
26. Jane B. Baron, *Property as Control: The Case of Information*, 18 MICHIGAN TELECOMMUNICATIONS AND TECHNOLOGY LAW REVIEW 367-418 (2012);
27. Jerome H. Reichman & Pamela Samuelson, *Intellectual Property Rights in Data?*, 50 VANDERBILT LAW REVIEW 52-166 (1997)
28. John Selby, *Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both?*, 25 INTERNATIONAL JOURNAL OF LAW AND INFORMATION TECHNOLOGY 213-232 (2017)
29. Jamie Lund, *Property Rights to Information*, 10 NORTHWESTERN JOURNAL OF TECHNOLOGY AND INTELLECTUAL PROPERTY 1-18 (2011)
30. Lawrence Lessig, *The Architecture of Privacy: Remaking Privacy in Cyberspace*, 1 VANDERBILT JOURNAL OF ENTERTAINMENT AND TECHNOLOGY LAW 56-65 (1999)

31. Lothar Determann, *No One Owns Data*, 70 HASTINGS LAW JOURNAL 1-44 (2019)
32. Lucas Bergkamp, *EU Data Protection Policy - The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-Driven Economy*, 18 COMPUTER LAW & SECURITY REVIEW: THE INTERNATIONAL JOURNAL OF TECHNOLOGY LAW AND PRACTICE 31-47 (2002)
33. Mandeep Kaur Saggi & Sushma Jain, *A Survey Towards an Integration of Big Data Analytics to Big Insights for Value-Creation*, 54 INFORMATION PROCESSING & MANAGEMENT 758-790 (2018)
34. María Verónica PEREZ ASINARI, *Is There any Room for Privacy and Data Protection within the WTO Rules?*, 9 ELECTRONIC COMMISSION LAW REVIEW 249-280 (2002)
35. Marshall Van Alstyne, Erik Brynjolfsson & Stuart Madnick, *Why Not One Big Database? Principles for Data Ownership*, 15 DECISION SUPPORT SYSTEMS 267-284 (1995)
36. Meng Lu, *Intellectual Property Protection of Big Data*, 1693 JOURNAL OF PHYSICS: CONFERENCE SERIES 012012 (2020)
37. Mira Burri & Rahel Schär, *The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy*, 6 JOURNAL OF INFORMATION POLICY 479 (2016)
38. Mira Burri, *Interfacing Privacy and Trade*, 53 Case W. Res. J. Int'l L. 35 (2021), 53 CASE WESTERN RESERVE JOURNAL OF INTERNATIONAL LAW (2021)
39. Mugdha Ghotkar & Priyanka Rokde, *Big Data: How it is Generated and its Importance*, 2 IOSR JOURNAL OF COMPUTER ENGINEERING (IOSR-JCE) 1-5 (2016)
40. Nadezhda Purtova, *The Illusion of Personal Data as No One's Property*, 7 LAW, INNOVATION AND TECHNOLOGY 83-111 (2015)
41. Nivedita Sen, *Understanding the Role of the WTO in International Data Flows: Taking the Liberalization or the Regulatory Autonomy Path?*, 21 JOURNAL OF INTERNATIONAL ECONOMIC LAW 323-348 (2018)
42. Oliver Diggelmann & Maria N. Cleis, *How The Right To Privacy Became A Human Right*, 14 HUM. RTS. L. REV. 441, 446-47 (2014)



43. Omer Tene and Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 NW. J. TECH. & INTELL. PROP. 239 (2013)
44. Patricia Mell, *Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness*, 11 BERKELEY TECHNOLOGY LAW JOURNAL 1-92 (1996)
45. Patrik Hummel, Matthias Braun & Peter Dabrock, *Own Data? Ethical Reflections on Data Ownership*, 34 PHILOSOPHY & TECHNOLOGY 545-572 (2020)
46. Paul M. Schwartz, *Information Privacy in the Cloud*, 161 UNIVERSITY OF PENNSYLVANIA LAW REVIEW (2013)
47. Paul M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARVARD LAW REVIEW (2013)
48. Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA LAW REVIEW 1701 (2010)
49. Raymond T. Nimmer & Patricia A. Krauthaus, *Information as Property Databases and Commercial Property*, 1 INTERNATIONAL JOURNAL OF LAW AND INFORMATION TECHNOLOGY 3-34 (1993)
50. Richard Cumbley & Peter Church, *Is "Big Data" Creepy?*, 29 COMPUTER LAW & SECURITY REVIEW 601-609 (2013)
51. Richard Kemp, *Legal aspects of Managing Big Data*, 30 COMPUTER LAW & SECURITY REVIEW 482-491 (2014)
52. Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381, 2413 (1996)
53. Robert C. Ellickson, *Two Cheers for the Bundle-of-Sticks Metaphor, Three Cheers for Merrill and Smith*, 8 ECON JOURNAL WATCH 215-222 (2011)
54. Ryan Moshell, *And Then There Was One: The Outlook for a Self-Regulatory United States Amidst a Global Trend Towards Comprehensive Data Protection Framework*, 37 TEXAS TECH LAW REVIEW 357 (2005)
55. S. Yakovleva & K. Irion, *The Best of Both Worlds? Free Trade in Services and EU Law on Privacy and Data Protection*, 2 EUROPEAN DATA PROTECTION LAW REVIEW 191-208 (2016)
56. S. Yakovleva & K. Irion, *The Best of Both Worlds? Free Trade in Services and EU Law on Privacy and Data Protection*, 2 EUROPEAN DATA PROTECTION LAW REVIEW 191-208 (2016)

57. Safanaz Heidari et al., *Big data clustering with varied density based on MapReduce*, 6 JOURNAL OF BIG DATA (2019)
58. Shlomit Yanisky-Ravid & Luis Antonio Luis Antonio Velez- Hernandez, *Copyrightability of Artworks Produced by Creative Robots and Originality: The Formality-Objective Model*, 19 MINNESOTA JOURNAL OF LAW, SCIENCE & TECHNOLOGY (2018)
59. Shlomit Yanisky-Ravid & Samuel Moorhead, *Generating Rembrandt: Artificial Intelligence, Accountability and Copyright - The Human-Like Workers Are Already Here - A New Model*, 2017 MICHIGAN STATE LAW REVIEW 659 (2017)
60. Sjef van Erp, *Ownership of Data: The Numerus Clausus of Legal Objects*, BRIGHAM-KANNER PROPERTY RIGHTS CONFERENCE JOURNAL 235-257 (2017)
61. Susan Aaronson, *Why Trade Agreements are not Setting Information Free: The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights, and National Security*, 14 WORLD TRADE REVIEW 671-700 (2015)
62. Svetlana Yakovleva, *Personal Data Transfers in International Trade and EU Law: A Tale of Two 'Necessities'*, 21 THE JOURNAL OF WORLD INVESTMENT & TRADE 881-919 (2020)
63. Svetlana Yakovleva, *Privacy Protection(ism): The Latest Wave of Trade Constraints on Regulatory Autonomy*, 74 U. MIAMI L. REV. 416 (2020)
64. Teresa Scassa, *Sharing Data in the Platform Economy: A Public Interest Argument for Access to Platform Data*, 50 UBC LAW REVIEW 1017-1071 (2017)
65. Thomas W. Merrill & Henry E. Smith, *What Happened to Property in Law and Economics?*, 111 THE YALE LAW JOURNAL 357 (2001)
66. Tlacuilo Fuentes, Itzayana, *Legal Recognition of the Digital Trade in Personal Data*, MEXICAN LAW REVIEW, [S.l.], p. 87-117, dec. 2019.
67. V.K. Gupta, *Copyright Issues Relating to Database Use*, 17 DESLDOC BULLETIN OF INFORMATION TECHNOLOGY 11-16 (1997)
68. Václav Janeček, *Ownership of personal data in the Internet of Things*, 34 COMPUTER LAW & SECURITY REVIEW 1039-1052 (2018).
69. W. Gregory Voss, *Cross-Border Data Flows, the GDPR, and Data Governance*, 29 WASH. INT'L. L.J. 485 (2020)

70. William R. Vance, *The Restatement of the Law of Property*, 86 UNIVERSITY OF PENNSYLVANIA LAW REVIEW AND AMERICAN LAW REGISTER 173 (1937)
71. Yassir Elrayah, *Big Data: Intellectual Property and Legal Issues*, 1 IMPACT: JOURNAL OF DIGITAL INFORMATION TECHNOLOGY (2016)

## INTERNET SOURCES

1. Adrienn Lukács, *What Is Privacy? The History and Definition of Privacy* (2016), <http://publicatio.bibl.u-szeged.hu/10794/7/3188699.pdf> (last visited Sep 29, 2021)
2. Annie Sorbie et al., *Does data ownership hinder biomedical research? Liminal Spaces Policy Brief* (2020), <http://Does data ownership hinder biomedical research? Liminal Spaces Policy Brief> (last visited Sep 30, 2021)
3. Chana Rungrojtanakul, *Legal Protection of Sui Generis Databases*, 2005, <https://digitalcommons.law.ggu.edu/cgi/viewcontent.cgi?article=1015&context=theses> (last visited Sep 30, 2021)
4. Claudia Jamin, *Managing Big Data in the Digital Age: An Industry Perspective, Intellectual Property and Digital Trade in the Age of Artificial Intelligence and Big Data* 150 (2018), [https://static-curis.ku.dk/portal/files/203882663/ceipi\\_ictsd\\_issue\\_5\\_final\\_0.pdf](https://static-curis.ku.dk/portal/files/203882663/ceipi_ictsd_issue_5_final_0.pdf) (last visited Sep 30, 2021)
5. Claudia Milbradt, *Global Intellectual Property Newsletter –23rd Edition – Legal Issues Surrounding the Protection of 'Data' and other IP Topics*, Clifford Chance (2019), <https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2019/09/global-intellectual-property-newsletter-23rd-edition-legal-issues-surrounding-the-protection-of-data-and-other-ip-t.pdf> (last visited Sep 30, 2021)
6. Consolidated Version of the Treaty on the Functioning of the European Union, October 26, 2012 O.J. (C 326) 47–390. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN>
7. Corien Prins, *When Personal Data, Behavior and Virtual Identities Become a Commodity: Would a Property Rights Approach Matter?*, 3 SCRIPT-ed 270-303 (2006)

8. David Reinsel, John Gantz & John Rydning, Data Age 2025: The Evolution of Data to Life-Critical Don't Focus on Big Data; Focus on the Data That's Big, An IDC White Paper Sponsored by Seagate (2017), <https://www.import.io/wp-content/uploads/2017/04/Seagate-WP-DataAge2025-March-2017.pdf> (last visited Oct 1, 2021)
9. Deloitte LLP, Realising the economic potential of machine-generated, non-personal data in the EU (2018), [https://www.vodafone.com/content/dam/vodcom/files/public-policy/Realising\\_the\\_potential\\_of\\_IoT\\_data\\_report\\_for\\_Vodafone.pdf](https://www.vodafone.com/content/dam/vodcom/files/public-policy/Realising_the_potential_of_IoT_data_report_for_Vodafone.pdf) (last visited Sep 30, 2021)
10. Ian Mitchell, The White Book of Big Data (2012), <https://www.fujitsu.com/se/imagesgig5/WhiteBookofBigData.pdf> (last visited Oct 1, 2021)
11. International and Comparative Legal Study on Big Data, WRR Working Paper 20, 'Big Data, Privacy and Security', Netherlands Scientific Council for Government Policy (WRR), (2016), <https://english.wrr.nl/publications/working-papers/2016/04/28/international-and-comparative-legal-study-on-big-data> (last visited Oct 1, 2021)
12. International Working Group on Data Protection in Telecommunications, Working Paper on Big Data and Privacy principles under pressure in the age of Big Data analytics, (2014)
13. James Manyika et al., Big Data: The Next Frontier for Innovation, Competition, And Productivity, McKinsey Global Institute (2011)
14. James Manyika et al., Digital Globalization: The New Era of Global Flows (2016), <https://www.mckinsey.com/~media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20globalization%20The%20new%20era%20of%20global%20flows/MGI-Digital-globalization-Full-report.ashx> (last visited Sep 29, 2021)
15. Jeroen van den Hoven et al., Privacy and Information Technology, in Stanford Encyclopedia of Philosophy (Edward N. Zalta 2019), <https://plato.stanford.edu/archives/win2019/entries/it-privacy/> (last visited Sep 30, 2021)

16. Liran Einav and Jonathan Levin, “The Data Revolution and Economic Analysis,” Working Paper, No. 19035, National Bureau of Economic Research, 2013
17. Max Competition, Arguments Against “Data Ownership” - Max Planck Institute for Innovation and Competition Max Planck Institute for Innovation and Competition,  
[https://www.ip.mpg.de/fileadmin/ipmpg/content/forschung/Argumentarium-Dateneigentum\\_eng.pdf](https://www.ip.mpg.de/fileadmin/ipmpg/content/forschung/Argumentarium-Dateneigentum_eng.pdf) (last visited Sep 30, 2021).
18. Meeting the Challenge of Big Data: Part One, (2012),  
<https://www.oracle.com/webfolder/s/assets/ebook/bigdata/index.html> (last visited Oct 1, 2021)
19. Michael Mandel, The Economic Impact of Data: Why Data Is Not Like Oil (2017). [https://www.progressivepolicy.org/wp-content/uploads/2017/07/PowerofData-Report\\_2017.pdf](https://www.progressivepolicy.org/wp-content/uploads/2017/07/PowerofData-Report_2017.pdf)
20. National Science Foundation, Solicitation 12-499: Core Techniques and Technologies for Advancing Big Data Science & Engineering (BIGDATA), 2012
21. Nationalsecurityforum.org, <https://nationalsecurityforum.org/wp-content/uploads/2018/01/NSS-Final-12-18-2017-0905-2.pdf> (last visited Sep 29, 2021).
22. Paven Malhotra, How Big Data and IP Intersect Big Data is big business—but who owns it?, Intellectual Property an ALM Supplement to Corporate Counsel, 2016,  
[https://www.keker.com/Templates/media/files/Articles/How%20Big%20Data%20and%20IP%20Intersect\\_Malhotra.pdf](https://www.keker.com/Templates/media/files/Articles/How%20Big%20Data%20and%20IP%20Intersect_Malhotra.pdf) (last visited Sep 30, 2021)
23. Richard M. Assmus, Mark Prinsley & Lana Khoury, IP Rights for Data: Mortaring Over the Cracks, (2019), <https://www.mayerbrown.com/-/media/files/perspectives-events/events/2019/07/event190723chiwebinarttiprightsslides.pdf> (last visited Sep 30, 2021)
24. Robert D. Atkinson, IP Protection in the Data Economy: Getting the Balance Right on 13 Critical Issues (2019), [https://www2.itif.org/2019-ip-protection-data-economy.pdf?\\_ga=2.177242277.1647718639.1632912651-1493660189.1632912651](https://www2.itif.org/2019-ip-protection-data-economy.pdf?_ga=2.177242277.1647718639.1632912651-1493660189.1632912651) (last visited Sep 30, 2021)
25. Software & Information Industry Association, White Paper on Data-Driven Innovation A Guide for Policymakers: Understanding and Enabling the Economic

- and Social Value of Data (2013),  
<https://history.siiia.net/Portals/0/pdf/Policy/Data%20Driven%20Innovation/data-driven-innovation.pdf> (last visited Oct 2, 2021)
26. Teresa Scassa, Data Ownership, CIGI Paper No. 187 (2018),  
<https://www.cigionline.org/publications/data-ownership/> (last visited Sep 30, 2021)
27. Top Big Data Analytics Use Cases, (2020),  
<https://www.oracle.com/a/ocom/docs/top-22-use-cases-for-big-data.pdf> (last visited Oct 1, 2021); The IBM Big Data Platform, (2013),  
<https://tdwi.org/~media/692A428D271F4D648BF6732EF0120EC0.PDFDF&usg=AOvVaw1Z4hQ-jGAgNf4SQxBODnX8> (last visited Oct 1, 2021)
28. Wolfgang Kerber, A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis, MAGKS Joint Discussion Paper Series in Economics, No. 37-2016, Philipps-University Marburg, School of Business and Economics (2016), [https://www.uni-marburg.de/fb02/makro/forschung/magkspapers/paper\\_2016/37-2016\\_kerber.pdf](https://www.uni-marburg.de/fb02/makro/forschung/magkspapers/paper_2016/37-2016_kerber.pdf) (last visited Sep 30, 2021)
29. World Economic Forum, Big Data, Big Impact: New Possibilities for International Development (2012),  
[https://www3.weforum.org/docs/WEF\\_TC\\_MFS\\_BigDataBigImpact\\_Briefing\\_2012.pdf](https://www3.weforum.org/docs/WEF_TC_MFS_BigDataBigImpact_Briefing_2012.pdf) (last visited Oct 1, 2021)
30. Xiaomeng Su, Introduction to Big Data, Institutt for informatikk og e-l ring ved NTNU (2018), <https://lagesoft.files.wordpress.com/2018/11/bd-introduction-to-big-data.pdf> (last visited Oct 1, 2021)
31. Zhen Zhang, Personal Data Protection within WTO's Trade Framework.  
<https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjVzInx5aPzAhXn93MBHRA9Cf4QFnoECAIQAQ&url=https%3A%2F%2Fscripties.uba.uva.nl%2Fdownload%3Ffid%3Dc1413888&usg=AOvVaw00r65tbH5iWUVDzaI0PAhP> (last accessed Sep 29, 2021)

## WEBSITES

1. Adam Satariano, G.D.P.R., a New Privacy Law, Makes Europe World's Leading Tech Watchdog (Published 2018) *Nytimes.com* (2018),

- <https://www.nytimes.com/2018/05/24/technology/europe-gdpr-privacy.html> (last visited Sep 29, 2021)
2. Adam Schwartz, The Payoff From California’s “Data Dividend” Must Be Stronger Privacy Laws Electronic Frontier Foundation (2019), <https://www.eff.org/deeplinks/2019/02/payoff-californias-data-dividend-must-be-stronger-privacy-laws> (last visited Sep 30, 2021)
  3. Agreement on Trade-Related Aspects of Intellectual Property Rights, (1995) [https://www.wto.org/english/docs\\_e/legal\\_e/31bis\\_trips\\_01\\_e.htm](https://www.wto.org/english/docs_e/legal_e/31bis_trips_01_e.htm) (last visited Sep 30, 2021)
  4. Ashi Bhat and Suneeth Katarki, The Debate – Data Localization and Its Efficacy - Privacy - India, Mondaq.com (2018), <https://www.mondaq.com/india/privacy-protection/736934/the-debate-data-localization-and-its-efficacy> (last visited Sep 29, 2021)
  5. Bernard Marr, A brief history of big data everyone should read World Economic Forum (2015), <https://www.weforum.org/agenda/2015/02/a-brief-history-of-big-data-everyone-should-read/> (last visited Oct 1, 2021)
  6. Big Data Analytics, IBM, <https://www.ibm.com/in-en/analytics/hadoop/big-data-analytics> (last visited Oct 1, 2021)
  7. Big Data and Data Protection, <https://rm.coe.int/big-data-and-data-protection-ico-information-commissioner-s-office/1680591220> (last visited Sep 30, 2021)
  8. Big Data: What it is and why it matters, Sas.com, [https://www.sas.com/en\\_us/insights/big-data/what-is-big-data.html](https://www.sas.com/en_us/insights/big-data/what-is-big-data.html) (last visited Oct 1, 2021)
  9. Big Data: What it is and why it matters. [https://www.sas.com/en\\_us/insights/big-data/what-is-big-data.html](https://www.sas.com/en_us/insights/big-data/what-is-big-data.html)
  10. Carine Alexis, The Future of Data: Ownership, Application, AI, and New Roles Movableink.com (2018), <https://movableink.com/blog/the-future-of-data-ownership-application-ai-and-new-roles> (last visited Sep 30, 2021)
  11. China's Cybersecurity Law: Data Cross-Border Transfer, Protiviti.com, <https://www.protiviti.com/SG-en/insights/pov-data-cross-border-transfer> (last visited Sep 29, 2021)
  12. Copyright, Wipo.int, <https://www.wipo.int/copyright/en/> (last visited Sep 30, 2021)

13. Cross-Border Data Transfer and Data Localization Requirements in China, ISACA, <https://www.isaca.org/resources/news-and-trends/industry-news/2021/cross-border-data-transfer-and-data-localization-requirements-in-china> (last visited Sep 29, 2021).
14. Data Protection, European Free Trade Association, Efta.int, <https://www.efta.int/EEA/Data-Protection-505036> (last visited Sep 29, 2021)
15. Database rights: the basics, Pinsent Masons (2019), <https://www.pinsentmasons.com/out-law/guides/database-rights-the-basics> (last visited Sep 30, 2021)
16. David Scholte, EU Data Protection in Trade Agreements KSLR EU Law Blog (2021), <https://blogs.kcl.ac.uk/kslreuropeanlawblog/?p=1524> (last visited Sep 29, 2021)
17. Definition of Big Data - Gartner Information Technology Glossary, Gartner, <https://www.gartner.com/en/information-technology/glossary/big-data> (last visited Oct 1, 2021)
18. Digital trade - OECD, Oecd.org, <https://www.oecd.org/trade/topics/digital-trade/> (last visited Sep 29, 2021)
19. Frequently Asked Questions: Copyright, wipo.int, [https://www.wipo.int/copyright/en/faq\\_copyright.html](https://www.wipo.int/copyright/en/faq_copyright.html) (last visited Sep 30, 2021)
20. ISO/IEC 2382-1:1993(en) Information technology, Iso.org, <https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:-1:en> (last visited Oct 1, 2021)
21. J. Steven Perry, What is big data? More than volume, velocity and variety... IBM Developer Blog (2017), <https://developer.ibm.com/blogs/what-is-big-data-more-than-volume-velocity-and-variety/> (last visited Oct 1, 2021)
22. Jim Harper, Perspectives on property rights in data www.aei.org (2019), <https://www.aei.org/technology-and-innovation/perspectives-on-property-rights-in-data/> (last visited Sep 30, 2021)
23. John Hull, Protecting trade secrets: how organizations can meet the challenge of taking “reasonable steps”, WIPO Magazine, 2019, [https://www.wipo.int/wipo\\_magazine/en/2019/05/article\\_0006.html](https://www.wipo.int/wipo_magazine/en/2019/05/article_0006.html) (last visited Sep 30, 2021)
24. Keith D. Foote, A Brief History of Big Data DATAVERSITY (2017), <https://www.dataversity.net/brief-history-big-data/> (last visited Oct 1, 2021)



25. Law in United States - DLA Piper Global Data Protection Laws of the World, Dlapiperdataprotection.com (2021), <https://www.dlapiperdataprotection.com/index.html?t=law&c=US&c2=> (last visited Sep 29, 2021)
26. Leslie Johnston, How many Libraries of Congress does it take?" The Signal: Digital Preservation Library of Congress (2012), <https://blogs.loc.gov/thesignal/2012/03/how-many-libraries-of-congress-does-it-take/>. (last visited Oct 2, 2021)
27. Liam Tung, Microsoft: We're giving you all Euro-style GDPR rights over how we use your data, ZDNet ZDNet (2018), <https://www.zdnet.com/article/microsoft-were-giving-you-all-euro-style-gdpr-rights-over-how-we-use-your-data/> (last visited Sep 29, 2021)
28. Lora Mourcous, Ownership of Personal Data under Dutch law? SOLV (2020), <https://solv.nl/en/blog/ownership-of-personal-data-in-dutch-law/> (last visited Sep 30, 2021)
29. Malcolm Crompton & Peter Ford, Implementing the APEC Privacy Framework: A New Approach Iapp.org (2005), <https://iapp.org/news/a/2005-12-implementing-the-apec-privacy-framework-a-new-approach/> (last visited Sep 29, 2021)
30. Mark Beyer & Douglas Laney, The Importance of 'Big Data': A Definition, Gartner (2012), Available at <http://www.gartner.com/doc/2595417>
31. Mark Hall, Amazon.com | History & Facts Encyclopedia Britannica, <https://www.britannica.com/topic/Amazoncom> (last visited Sep 30, 2021)
32. Mark Hall, Facebook | Overview, History, & Facts Encyclopedia Britannica (2021), <https://www.britannica.com/topic/Facebook> (last visited Sep 30, 2021).
33. Martina F. Ferracane, Janez Kren, Erik van der Marel, The Cost of Data Protectionism, ECIPE (2018), <https://ecipe.org/blog/the-cost-of-data-protectionism/> (last visited Sep 29, 2021)
34. Mehreen Khan & Tim Bradshaw, Apple and Facebook call for EU-style privacy laws in US Ft.com (2018), <https://www.ft.com/content/0ca8466c-d768-11e8-ab8e-6be0dcf18713> (last visited Sep 29, 2021)
35. Michael Wu, Big Data Analytics: Turning Zettabytes of Data into Actionable Information MyCustomer (2012), <https://www.mycustomer.com/marketing/data/big-data-analytics-turning-zettabytes-of-data-into-actionable-information> (last visited Oct 1, 2021)

36. Mike Gualtieri, The Pragmatic Definition of Big Data Forrester (2012),  
[https://www.forrester.com/blogs/12-12-05-the\\_pragmatic\\_definition\\_of\\_big\\_data/](https://www.forrester.com/blogs/12-12-05-the_pragmatic_definition_of_big_data/)  
 (last visited Oct 1, 2021)
37. Nigel Cory, Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost? Itif.org (2021), <https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost> (last visited Sep 29, 2021)
38. Notice of the People's Bank of China on Printing and Distributing the “Implementation Measures for the Protection of the Rights and Interests of Financial Consumers of the People's Bank of China”\_State Council Communiqué No. 21 of 2017\_Chinese Government Website, Gov.cn,  
[http://www.gov.cn/gongbao/content/2017/content\\_5213211.htm](http://www.gov.cn/gongbao/content/2017/content_5213211.htm) (last visited Sep 29, 2021)
39. Notice of the State Internet Information Office on the Public Consultation on the “Measures for the Security Evaluation of the Exit of Personal Information and Important Data (Draft for Solicitation of Comments)”-Office of the Central Committee of the Communist Party of China Cyber Security and Information Technology, Cac.gov.cn, [http://www.cac.gov.cn/2017-04/11/c\\_1120785691.htm](http://www.cac.gov.cn/2017-04/11/c_1120785691.htm) (last visited Sep 29, 2021)
40. People's Bank of China (PBOC), Financial Data Security Data Lifecycle Security Specification, China, Hankunlaw.com,  
<https://www.hankunlaw.com/downloadfile/newsAndInsights/c4b38d77b09fc65076a94458637c0e35.pdf> (last visited Sep 29, 2021)
41. Peter Leonard, Beyond Data Privacy: Data “Ownership” and Regulation of Data-Driven Business americanbar.org (2020),  
[https://www.americanbar.org/groups/science\\_technology/publications/scitech\\_lawyer/2020/winter/beyond-data-privacy-data-ownership-and-regulation-datadriven-business/](https://www.americanbar.org/groups/science_technology/publications/scitech_lawyer/2020/winter/beyond-data-privacy-data-ownership-and-regulation-datadriven-business/) (last visited Sep 30, 2021)
42. Policies.google.com, <https://policies.google.com/technologies/partner-sites?hl=en-US> (last visited Sep 30, 2021)
43. Samuel Coldicutt and Nivedita Sen, Testing the GDPR's WTO readiness Linklaters, <https://www.linklaters.com/en/insights/blogs/tradelinks/testing-the-gdprs-wto-readiness> (last visited Sep 29, 2021)

44. Samuel Cristobal, Two more V's in Big Data: Veracity and Value - DATASCIENCE Datascience.aero (2020), <https://datascience.aero/big-data-veracity-value/> (last visited Oct 1, 2021)
45. Stephen Baker, Big Data and Math Thenumerati.net (2012), <http://thenumerati.net/?postID=845&big-data-and-math> (last visited Sep 30, 2021)
46. Steve Lohr, The Age of Big Data, The New York Times, 2012, <https://www.nytimes.com/2012/02/12/sunday-review/big-datas-impact-in-the-world.html> (last visited Oct 1, 2021)
47. Thomas M. Boyd & Tara Sugiyama Potashnik, Data Ownership - The Suitability of a Consumer Property Right in a 21st Century Economy (2020), <https://www.venable.com/insights/publications/2020/09/data-ownership> (last visited Sep 30, 2021)
48. Trade Secrets Protection and Incentives to Innovate: Scrutinizing Section 91 of The Personal Data Protection Bill, 2019, SpicyIP (2020), <https://spicyip.com/2020/07/trade-secrets-protection-and-incentives-to-innovate-scrutinizing-section-91-of-the-personal-data-protection-bill-2019.html> (last visited Sep 30, 2021)
49. Trade Secrets, wipo.int, <https://www.wipo.int/tradesecrets/en/> (last visited Sep 30, 2021)
50. Translation: Critical Information Infrastructure Security Protection Regulations (Effective Sept. 1, 2021), DigiChina, <https://digichina.stanford.edu/news/translation-critical-information-infrastructure-security-protection-regulations-effective-sept> (last visited Sep 29, 2021)
51. Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017), New America, <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/> (last visited Sep 29, 2021)
52. Translation: Data Security Law of the People's Republic of China, DigiChina, <https://digichina.stanford.edu/news/translation-data-security-law-peoples-republic-china> (last visited Sep 29, 2021)
53. Translation: New Draft Rules on Cross-Border Transfer of Personal Information Out of China, New America, <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-new-draft-rules-cross-border-transfer-personal-information-out-china/> (last visited Sep 29, 2021)

54. Translation: Personal Information Protection Law of the People's Republic of China (Effective Nov. 1, 2021), DigiChina, <https://digichina.stanford.edu/news/translation-personal-information-protection-law-peoples-republic-china-effective-nov-1-2021> (last visited Sep 29, 2021)
55. Vindu Goel, India Pushes Back Against Tech ‘Colonization’ by Internet Giants (Published 2018) Nytimes.com (2018), <https://www.nytimes.com/2018/08/31/technology/india-technology-american-giants.html> (last visited Sep 29, 2021)
56. Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2025(in zettabytes), Statista (2021), <https://www.statista.com/statistics/871513/worldwide-data-created/> (last visited Oct 1, 2021)
57. What Is Big Data? | Oracle, Oracle.com, <https://www.oracle.com/big-data/what-is-big-data/> (last visited Oct 1, 2021)
58. Who owns the Machine Generated Data in IoT – Men or Machine?, IIoT World (2017), <https://www.iiot-world.com/industrial-iot/digital-disruption/who-owns-the-machine-generated-data-in-iot-men-or-machine/> (last visited Sep 30, 2021)
59. WIPO Copyright Treaty (WCT) (1996), <https://wipolex.wipo.int/en/text/295157> (last visited Sep 30, 2021)
60. WTO | Intellectual Property - Overview of TRIPS Agreement, wto.org, [https://www.wto.org/english/tratop\\_e/trips\\_e/intel2\\_e.htm](https://www.wto.org/english/tratop_e/trips_e/intel2_e.htm) (last visited Sep 30, 2021)

## **REPORTS**

1. Australian Law Reform Commission, For Your Information: Australian Privacy Law and Practice (2008), <https://www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/31-cross-border-data-flows/introduction-139/> (last visited Sep 29, 2021)
2. Basic Proposal for the Substantive Provisions of the Treaty on Certain Questions Concerning the Protection of Literary and Artistic Works to be considered by the Diplomatic Conference CRNR/DC/4, In Diplomatic Conference on Certain Copyright and Neighboring Rights Questions (1996),

- [https://www.wipo.int/edocs/mdocs/diplconf/en/crn\\_r\\_dc/crn\\_r\\_dc\\_4.pdf](https://www.wipo.int/edocs/mdocs/diplconf/en/crn_r_dc/crn_r_dc_4.pdf) (last visited Sep 30, 2021).
3. *Big Data: Seizing Opportunities, Preserving Value* (2014), [https://obamawhitehouse.archives.gov/sites/default/files/docs/big\\_data\\_privacy\\_report\\_may\\_1\\_2014.pdf](https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf) (last visited Oct 1, 2021)
  4. COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation COM/2020/264 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0264&from=EN>
  5. Congressional Research Service, U.S.-EU Privacy Shield (2021), <https://www.everycrsreport.com/reports/IF11613.html>. (last visited Sep 29, 2021)
  6. David Coffin & et al, United States International Trade Commission, Global Digital Trade I: Market Opportunities and Key Foreign Trade Restrictions (2017), <https://www.usitc.gov/publications/332/pub4716.pdf> (last visited Sep 29, 2021).
  7. EDPS/2021/03, Data protection is non-negotiable in international trade, [https://edps.europa.eu/system/files/2021-02/edps-2021-03-tca\\_uk\\_en.pdf](https://edps.europa.eu/system/files/2021-02/edps-2021-03-tca_uk_en.pdf)
  8. Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies, Directorate for Science, Technology and Innovation, OECD Publishing, Paris (2019)
  9. European Commission, Building A European Data Economy (2017), <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0009&from=EN> (last visited Sep 30, 2021)
  10. European Commission, Commission Staff Working Document on the free flow of data and emerging issues of the European data economy Accompanying the document Communication Building a European data economy {COM(2017) 9 final} (2017), [https://ec.europa.eu/newsroom/dae/document.cfm?doc\\_id=41247](https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41247) (last visited Sep 30, 2021); See also, European Commission, Building A European Data Economy {SWD(2017) 2 final} (2017), <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0009&from=EN> (last visited Sep 30, 2021).

11. Francesca Casalinii & Javier López González, Trade and Cross-Border Data Flows, OECD Trade Policy Papers (2019), [https://www.oecd-ilibrary.org/trade/trade-and-cross-border-data-flows\\_b2023a47-en](https://www.oecd-ilibrary.org/trade/trade-and-cross-border-data-flows_b2023a47-en) (last visited Sep 29, 2021)
12. Graham Greenleaf, Convention 108+ and the Data Protection Framework of the EU (Speaking Notes for Conference Presentation), Convention 108+ Tomorrow's Common Ground for Protection' (Council of Europe, Strasbourg, 21 June 2018). UNSW Law Research Paper No. 18-39 (2018)
13. IAPP–EY Annual Governance Report (2019), [http://startupoba.com.br/portaldaprivacidade.com.br/wp-content/uploads/attachments/28563d\\_01043d7b2e454271b15caf16d548a741.pdf](http://startupoba.com.br/portaldaprivacidade.com.br/wp-content/uploads/attachments/28563d_01043d7b2e454271b15caf16d548a741.pdf) (last accessed Sep 29, 2021)
14. Josef Drexler et al., 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 & Competition Research Paper No. 16-10 (2016)
15. Josef Drexler et al., Position Statement of the Max Planck Institute for Innovation and Competition of 26 April 2017 on the European Commission's 'Public consultation on Building the European Data Economy', Max Planck Institute for Innovation & Competition Research Paper No. 17-08 (2017)
16. Mark Begor, Written Testimony, in Hearing: Who's Keeping Score? Holding Credit Bureaus Accountable and Repairing a Broken System, Committee on Financial Services U.S. House of Representatives (2019), <https://docs.house.gov/meetings/BA/BA00/20190226/108945/HHRG-116-BA00-Wstate-BegorM-20190226.pdf> (last visited Sep 30, 2021)
17. Martin Fadler & Christine Legner, Who Owns Data in the Enterprise? Rethinking Data Ownership in times of Big Data and Analytics, in 28th European Conference on Information Systems (ECIS) (2020)
18. Meglena Kuneva, Keynote Speech, in Roundtable on Online Data Collection, Targeting and Profiling 2 (2009), [https://ec.europa.eu/commission/presscorner/detail/en/SPEECH\\_09\\_156](https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_09_156) (last visited Sep 30, 2021)

19. Nestor Duch-Brown, Bertin Martens & Frank Mueller-Langer, *The Economics of Ownership, Access and Trade in Digital Data* (2017), <https://ec.europa.eu/jrc/sites/default/files/jrc104756.pdf> (last visited Sep 30, 2021)
20. OECD (2011-04-06), “The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines”, *OECD Digital Economy Papers*, No. 176, OECD Publishing, Paris. <http://dx.doi.org/10.1787/5kgf09z90c31-en>
21. Rachel F. Fefer, Congressional Research Service, R45584, *Data Flows, Online Privacy, and Trade Policy*(2020)
22. The Ministry of Electronics & Information Technology (MeitY), *Report by the Committee of Experts on Non-Personal Data Governance Framework* (2020), <https://ourgovdotin.files.wordpress.com/2020/12/revised-report-kris-gopalakrishnan-committee-report-on-non-personal-data-governance-framework.pdf> (last visited Sep 30, 2021)
23. U.S. Trade Representative, *2018 National Trade Estimate Report on Foreign Trade Barriers*, 2018, [https://ustr.gov/sites/default/files/files/Press/Reports/2018%20National%20Trade%20Estimate%20Report.pdf?utm\\_source=POLITICO.EU&utm\\_campaign=f17a177eee-EMAIL\\_CAMPAIGN\\_2018\\_04\\_02&utm\\_medium=email&utm\\_term=0\\_10959edeb5-f17a177eee-189017913](https://ustr.gov/sites/default/files/files/Press/Reports/2018%20National%20Trade%20Estimate%20Report.pdf?utm_source=POLITICO.EU&utm_campaign=f17a177eee-EMAIL_CAMPAIGN_2018_04_02&utm_medium=email&utm_term=0_10959edeb5-f17a177eee-189017913)
24. UN, GENERAL ASSEMBLY, REVISED DRAFT RESOLUTION ON THE RIGHT TO PRIVACY IN THE DIGITAL AGE, A/C.3/71/L.39/ REV.1, NEW YORK, 16 NOVEMBER 2016, [https://digitallibrary.un.org/record/848969/files/A\\_C-3\\_71\\_L-39\\_Rev-1-EN.pdf](https://digitallibrary.un.org/record/848969/files/A_C-3_71_L-39_Rev-1-EN.pdf); UN, HUMAN RIGHTS COUNCIL, THE RIGHT TO PRIVACY IN THE DIGITAL AGE (2017), A/HRC/34/L.7/REV.1, <https://documents-dds-ny.un.org/doc/UNDOC/LTD/G17/073/06/PDF/G1707306.pdf?OpenElement>.
25. UNCTAD, *Data Protection and Privacy Legislation Worldwide*, [unctad.org](https://unctad.org/page/data-protection-and-privacy-legislation-worldwide), <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide> (last accessed Sep 29, 2021)
26. Ustr.gov, <https://ustr.gov/sites/default/files/Digital-2-Dozen-Updated.pdf> (last visited Sep 29, 2021)


## APPENDIX

### THE NATIONAL UNIVERSITY OF ADVANCED LEGAL STUDIES Kalamassery, Kochi – 683 503, Kerala, India

#### CERTIFICATE ON PLAGIARISM CHECK

1.	Name of the Candidate	Mr. S. Muhammad Ali Khan
2.	Title of thesis/dissertation	IP Ownership and Protection - An Analysis
3.	Name of the supervisor	Dr. Anil R. Nair
4.	Similar content (%) identified	4%
5.	Acceptable maximum limit (%)	10%
6.	Software used	OURGINAL (URKUND)
7.	Date of verification	11 October 2021

*\*Report on plagiarism check, specifying included/excluded items with % of similarity to be attached in the Appendix*

Checked By (with name, designation & signature)	Dr. Anil R. Nair, Associate Professor	
Name and Signature of the Candidate	Mr. S. Muhammad Ali Khan	
Name & Signature of the Supervisor	Dr. Anil R. Nair, Associate Professor	