Personal Data Monetisation Strategy: Systematic Review and a Case Study of UAE

استراتيجية تحويل البيانات الشخصية إلى قيمة اقتصادية: دراسة تحليلية و دراسة حالة دولة الإمارات العربية المتحدة

by

REEM AL FALASI

Dissertation submitted in fulfilment

of the requirements for the degree of

MSc INFORMATICS

at

The British University in Dubai

July 2019

DECLARATION

I warrant that the content of this research is the direct result of my own work and that any use made in it of published or unpublished copyright material falls within the limits permitted by international copyright conventions.

I understand that a copy of my research will be deposited in the University Library for permanent retention.

I hereby agree that the material mentioned above for which I am author and copyright holder may be copied and distributed by The British University in Dubai for the purposes of research, private study or education and that The British University in Dubai may recover from purchasers the costs incurred in such copying and distribution, where appropriate.

I understand that The British University in Dubai may make a digital copy available in the institutional repository.

I understand that I may apply to the University to retain the right to withhold or to restrict access to my thesis for a period which shall not normally exceed four calendar years from the congregation at which the degree is conferred, the length of the period to be specified in the application, together with the precise reasons for making that application.

_____

Signature of the student

COPYRIGHT AND INFORMATION TO USERS

The author whose copyright is declared on the title page of the work has granted to the British University in Dubai the right to lend his/her research work to users of its library and to make partial or single copies for educational and research use.

The author has also granted permission to the University to keep or make a digital copy for similar use and for the purpose of preservation of the work digitally.

Multiple copying of this work for scholarly purposes may be granted by either the author, the Registrar or the Dean only.

Copying for financial gain shall only be allowed with the author's express permission.

Any use of this work in whole or in part shall respect the moral rights of the author to be acknowledged and to reflect in good faith and without detriment the meaning of the content, and the original authorship.

Abstract

Governments are always looking for an improved vision which enhances construction of citizens' quality of life. This vision can be achieved through governmental data monetisation to determine citizens' challenges and demands. The monetisation procedure will lead to reduction of the city's expenses, inspire innovation, and encourage economic growth. However, currently, there is a lack of a practical governmental data strategy or related processes and platforms. Furthermore, data providers have several concerns regarding their shared data, as they have no control over or ownership rights to it. This purpose of this study is to 1) to investigate the elements necessary to build a targeted governmental data monetisation strategy, 2) explore the existing personal data monetisation procedures, and 3) recognise data providers' awareness of their data monetisation and the economic growth of this process in the UAE. The concept has been explored in order to answer the study's research questions though the literature review, systematic review of 182 works of research published between 2002 and 2019, and the UAE case study, which collected 225 responses from the conducted survey to investigate data providers' willingness to share their data and their knowledge of their data's commercial value. The key findings indicate that data providers require a trusting and confidential relationship with the data consumers, who monetise data from the business entities, and maintain the data providers' privacy and provide efficiency benefits across different entities. Future study will explore the governmental data monetisation strategy of a specific organisation in the UAE in addition to investigating the monetisation procedure from the data consumer's point of view.

Keywords: *United Arab Emirates, UAE citizens, Systematic Review, Governmental Data Monetisation Strategy, Data Monetisation Procedure, City data, Data Provider, Data Consumer, Data Trading, Data Economic Growth*

ملخص

تبحث الحكومات دائمًا عن الرؤية المبتكرة التي تؤدي إلى تحسين حياة المواطنين. سيتم تحقيق هذه الرؤية من خلال تحويل البيانات الحكومية إلى قيمة اقتصادية من أجل معرفة تحديات ومطالب المواطنين. تؤدي هذه العملية إلى نتيجة محققة من خلال خفض نفقات المدينة، وإلهام الابتكار وزيادة النمو الاقتصادي. ومع ذلك، هناك نقص في استراتيجية البيانات الحكومية المطبقة بالإضافة إلى العمليات والتطبيقات المتعلقة وذات صلة بهذه الاستراتيجية. كما أن مزودي البيانات لديهم العديد من المخاوف فيما يتعلق ببياناتهم، حيث لا يملكون أي حقوق في ملكية والتحكم في بياناتهم القيمة. الهدف من هذه الدراسة هو 1) هو التحقيق في العناصر اللازمة لبناء استراتيجية تحويل البيانات الحكومية إلى قيمة اقتصادية، 2) استكشاف إجراءات الأنظمة وتحويل البيانات الشخصية إلى قيمة اقتصادية الحالية، و3) للتعرف على مدى وعي مقدمي البيانات بتحويل بياناتهم الحكومية إلى قيمة اقتصادية والنمو الاقتصادي الناتج لهذه العملية في دولة الإمارات العربية المتحدة. وقد تم إجراء الاستكشاف من أجل الإجابة على أسئلة البحث من خلال مراجعة المؤلفات، والاستعراض المنهجي لـ 182 بحثًا تم نشرهم من 2002 إلى 2019، ودراسة الحالة في الإمارات العربية المتحدة التي جمعت 225 إجابة من المسح الذي تم إجراؤه لاستكشاف مدى رغبة مقدمي البيانات في مشاركة بياناتهم ومدى معرفتهم بالقيمة التجارية لهذه البيانات. تشير النتائج الرئيسية إلى أن موفري البيانات يحتاجون إلى علاقة موثوقة وسرية مع مستهلكي البيانات، الشركات التي تحقق الدخل من تحويل البيانات الحكومية إلى قيمة اقتصادية، فضلاً عن الحفاظ على خصوصية مزودي البيانات وتوفير المزايا والمنافع المتوقعة عبر مختلف المجالات. وسيستكشف العمل المستقبلي استراتيجية تحقيق الدخل من البيانات الحكومية في منظمة محددة في دولة الإمارات العربية المتحدة. بالإضافة إلى التحقيق في وجهة نظر مستهلكين البيانات من إجراء عملية تحويل البيانات الحكومية إلى قيمة اقتصادية.

Dedication

First, I want to thank God for every moment of joy and pleasure I am living with.

With all appreciation and gratefulness, I would like to dedicate my dissertation to my supportive family, friends, teachers, and work colleagues, who wished me luck and prayed for my success and excellence with all their love.

I’m blessed to be surrounded by a group of motivators who always encourage me to strive for success and surpass any obstacles.

Acknowledgement

This dissertation wouldn’t be effective and successful without the guidance of **Professor Sherief Abdallah**. I’m genuinely honoured to have received his teaching effort and supervision time as well as his valuable experience and infinite advice. I would also like to give a special thanks to **Professor Khaled Shaalan** who supported me from day one of my master journey.

This work couldn’t have been accomplished without the support of all those who encouraged, supported and believed in me with all their prayers and love.

Table of Contents

List of illustrations

List of Tables

List of Abbreviations

Abbreviation	Description
BI	Business Intelligence
CRM	Customer Relationship Management
DHC	Dubai Healthcare City
DIFC	Dubai International Financial Centre
DPR	Data Protection Regulations
EU	European Union
FSS	Federal Security Service
FSTEC	Federal Services for Technical and Export Control
GDPR	General Data Protection Regulation
IdMS	Identity Management System
IoT	Internet of Things
OECD	Organisation for Economic Co-operation and Development
PD	Personal Data
PDE	Personal Data Economy
PDPA	Personal Data Protection Act
PDS	Personal Data Store
PHD coin	Personal Health Data coin
PI	Personal Informatics
PIGEON	PersonalIzed web paGe rEcommendatiON
PII	Personally Identifiable Information
PoS	Point of Sale
ROI	Return on Investment

TRA	Telecommunications Regulatory Authority
UAE	United Arab Emirates
UK	United Kingdom
US	United States
WDSs	Web-based Data Services

1 Chapter One: Introduction

This chapter presents a background of the governmental data monetisation and its existing worldwide challenges. It also introduces the problem, motivations, and objectives of this paper. In addition, the research questions are also highlighted alongside the dissertation structure.

1.1 Background

Organisations are currently looking for new revenue opportunities. One of these opportunities is data monetisation – the process of transferring information-based products and services for different industries. In fact, the medical supplier Owens and Minor started to monetise data in the mid-1990s by selling business intelligence (BI) and analytics reports to their customers – hospitals and supply manufacturers (Tallon, Wixom & Buff 2015). Hence, most existing organisations today look for new revenue sources through data monetisation. However, data monetisation requires multiple capabilities and differs from traditional BI analytics tasks (Tallon, Wixom & Buff 2015).

As data keep growing by the second, the monetisation strategy keeps changing in order to provide enhanced services to customers. User's data have been valued at more than 300 billion euros; it is assumed that this value will increase threefold by 2020 (Hustinx 2014). There is significant attention on monetising individual identifying information to find all the impacted angles that drive innovated aspects across different industries (Tallon, Wixom & Buff 2015). Governmental data monetisation has a role in shaping modern business models and will lead to economic growth and enhance social security (Tallon, Wixom & Buff 2015).

Therefore, several studies have discussed an organisation's capability to aggregate and protect their customers' personal data and emphasised the organisation's ongoing practice of

monetising such data, as this concern is very critical from the customers' perspective (Johnson, Friend & Lee 2017; KPMG 2015; Information Builders 2018; Najjar & Kettinger 2013; Romualdo-Suzuki 2015; Tallon, Wixom & Buff 2015; Wilberg et al. 2017; Woerner & Wixom 2015).

1.2 Problem Description

Data is steadily growing. In fact, around 90% data has been created in the last two years and it is expected to rise by 27% yearly, mainly because of the evolution of the Internet of Things, (IoT) devices and the generated data volume (Sicari et al. 2015). Aligning with the data increase, the security and privacy aspects should also be considered.

Currently, most social or search engines platforms gather numerous different characteristics of each user's personal data (Plantin et al. 2018). However, these platforms occasionally collect their users' data with or without permission to provide special personalised services to their users. According to a recent study, 81% of social media users do not feel secure sharing their private data (Huddleston Jr 2014). Therefore, users have neither knowledge nor transparency regarding their monetised data. They also don't have any governance over their own shared personal data.

Furthermore, such platforms monetise user data for their benefits and generate revenue without sharing any profit with data producers (the users) (Li, Nirei & Yamana 2019). Collecting data is not an easy task for data consumers and providers (Bataineh et al. 2016). Data consumers need to find the right data provider, who provides qualified data. Furthermore, data consumers, the business entities who monetise the data, often have limited financial plans for data procurement and must choose the exact collection of data that meets their demand (Bataineh et al. 2016). In addition, data providers require data consumers who need their data as well as monetary knowledge about their data based on market demand to increase their profit

(Bataineh et al. 2016). There are some existing issues related to the data market, such as the lack of a unified platform to host all data providers (Bataineh et al. 2016). Individuals are compensated for sharing their data or for non-monetary rewards (Bataineh et al. 2016). Additionally, there is a lack of platforms that enable individuals to sell their data to data providers, like organisations who are responsible for such operations and benefit from them (Bataineh et al. 2016). Besides, lack of data classification is based on type and quality levels. Classification is required for each domain and to estimate the monetary value of each piece of data (Bataineh et al. 2016). The assumption of the data values is based on the time charge, change and market demand (Bataineh et al. 2016).

1.3 Motivation

There is a significant vision for building a data strategy for modern cities. Data is acknowledged as the infrastructure of wealth (Romualdo-Suzuki 2015). The purpose of data monetisation is to reduce countries' spends, motivate innovation, and increase economic growth (Romualdo-Suzuki 2015). The aim is to obtain an opportunity to retrieve all the benefits from the city's data market plan, work with a different kind of technical complexity challenge and enhance the required policies and regulations that suit the data evolution trend, for the purpose of generating win-win benefits and services for both the government and citizens. For instance, offering enhanced personalised services which lead to an increase in the generated governmental revenue.

There should be a potential to use the open "city data" to change the city and obtain the expected outcome (Tallon, Wixom & Buff 2015). Thus, there are three main elements that need to be considered: 1) the government should be aware and ready for the change that data will cause to their economy, strategy, and so on, 2) the ability to secure the generated data and willingness to contribute with the city's public and private sectors and 3) raising awareness and

building trust with people to encourage them to share their data, which will result in a new service to offer them (Tallon, Wixom & Buff 2015).

Moreover, there are four core alignments required to increase the city data values: 1) the city's data economy, such as city's public services, citizens awareness etc., needs to be simple and less complex for data providers (Romualdo-Suzuki 2015). Reducing complexity can be achieved by encouraging data sharing, interoperability, and overcoming security and privacy issues (Romualdo-Suzuki 2015) 2) building a city data market culture and encouraging it across the public and private sectors, 3) harmonizing the new created values and services across the developed data infrastructure, and 4) involving technical and non-technological elements such as business framework and data marketplace for equality along the data economy (Romualdo-Suzuki 2015).

Furthermore, the city's information can be gathered through the interaction between people and their social media feeds to share the city's/countries' information. Alkhatib, Barachi & Shaalan (2018) focused on retrieving Arabic feeds for information about any incident that occurred in the country. These feeds help rescuers such as police or fire-fighters to overcome issues in real time before they cause more danger to nearby citizens (Alkhatib, Barachi & Shaalan 2018).

1.4 Research Objectives

The governmental data monetisation process and strategy, particularly, play a significant role in our generation within different domains, characteristics, and industries. Thus, this study will explore the elements and factors required to build an effective data monetisation strategy within the city. It will also study the existing personal data monetisation strategies and procedures that have been implemented as well as their outcomes. In addition, it will investigate an individual's awareness of their personal data monetisation and their

knowledge about the generated value from such monetisation processes in the United Arab Emirates, (UAE), apart from highlighting individuals' acceptance to offer and share their personal data.

1.5 Research Questions

To meet the aims of this study, there are several questions to be asked and addressed, such as the following:

RQ1: What are the co-related definitions and common aims, problems, and challenges of the personal data monetisation process?

RQ2: What are the main factors that affect personal data monetisation along with the major related work and the common methodology used to monetise the personal data?

RQ3: What are the common outcomes of the personal data monetisation, as well as the main contexts in which personal data monetisation is used and the supported countries of personal data monetisation?

RQ4: What is the customer's main concerns about monetising their personal data and are the UAE's citizens aware of their personal data monetisation? (Case study)

1.6 Methodology

The methodology used in this study is a systematic review of the state-of-the-art aspects and domains related to personal data monetisation around the globe. In addition, this research will conduct a case study of the UAE in order to investigate individuals' awareness and knowledge of personal data monetisation as well as their willingness to provide their personal data. Hence, an online survey web link will be mailed and shared to all UAE citizens and the analysis of the collected responses will be highlighted and presented in this research.

1.7 Dissertation Structure

This dissertation is structured as follows:

Chapter one presents the background of the conducted study and the problem description, study motivation, and research objectives. The research questions and methodology are highlighted in order to meet the research objectives.

Chapter two highlights the literature review of the data monetisation overview, starting with data strategy structure including data types, the city's policy, changing cities' partners, strategic pathway, strategy themes, and data monetisation strategy frame along with its challenges, success factors, integration, and managers skills. It also discusses data monetisation business models including data monetisation procedures, impact, outcome, generating new revenue and emerging new products or services.

Chapter three presents the methodology used in order to achieve the study objectives. The methodology is based on the meta-analysis of high-ranked and relevant publications in the personal data monetisation domain within the three databases, Emerald Insight, IEEE, and Science Direct, and the Google Scholar search engine. This section will present the applied inclusion and exclusion criteria, data sources, and search strategies and quality assessment of the selected studies.

Chapter four presents the results along with their analysis discussion. Each highlighted research question is investigated through the scholar's publication collection. The related sub-topics of each question domain are also highlighted.

Chapter five illustrates the UAE case study results based on the conduct survey. It consists of the respondent's demographics data and research questionnaire results illustrated with figures and UAE citizens' opinions besides the overall case study discussion.

Chapter Six provide the study conclusion, recommendations, and research limitations, and ideas for further studies.

2 Chapter Two: Literature Review

This chapter presents the major aspects of data monetisation. It starts from the data strategy structure, including data types, city's policy, changing cities' partners, strategic pathway, strategy themes, and data monetisation strategy frame along with its challenges, succeed factors, integration, and managers skills. It also discusses data monetisation business models, including data monetisation procedures, impact, outcome, generating new revenue, and emerging new products or services.

2.1 Data Strategy Structure

2.1.1 Data Types

Data types are varied: 1) Open data: non-confidential and not private data published without any rules. 2) Private data: licensed data, not ready to provide value and requiring permission for access. 3) Commercial data: licensed data, has value and requires permission for access. 4) Sensory data: either open or restricted data gathered through varied types of sensors owned by the public, private sectors, or citizens. 5) Crowd-sourced data: data collected by users through online browsing and social media tools (Romualdo-Suzuki 2015).

Additionally, there are four types of data that one could get value from, such as 1) unstructured internal data, such as customer's text records and emails, 2) structured internal data such as sales, financial, and production data, 3) unstructured external data such as social media data and news, and 4) structured external data such as public market performance and demographics. The most value the organisation can get is by figuring out and exploring a relationship between different data types (KPMG 2015).

2.1.2 City's Policy

Data strategy should be aligned with city policy, including developing and managing city infrastructure, energy policy, border-smart city agenda, strategic decision-making at the city-level, better public services, proper digital government, city technology infrastructure, building citizens' trust and privacy, and, finally, promoting the city as a platform (Romualdo-Suzuki 2015).

2.1.3 Changing Cities' Partners

The data strategy direction is for three main groups who have a great role in the city data market: 1) structural partners who are actively involved with data strategy, e.g. open data institutes, public, and private services, and the Greater London Authority, (GLA), 2) supporting partners who provide services, equipment, and tools to validate the data strategy, and data publishers, e.g. telecoms, transport, and police authorities, and water, and energy utilities, 3) contributing partners who are frequent consumers of the data structure and authorised to create the business case and provide feedback (Romualdo-Suzuki 2015).

The two most important two partnership paths are: 1) data collaborators who add value to entity data to maximise the delivered value to customers and 2) a third party who acts as a distribution method when the organisation doesn't often deal with monetising data; as such, a third party is well-known for doing so in the specific domain that needs to be monetised (KPMG 2015).

Tallon, Wixom & Buff (2015) have consolidated techniques to analyse the collected transcript data of interviews regarding data monetisation approaches with 58 executives at 34 companies to obtain essential theories, interactions, and relationships that aim to form the best-practice methodologies in data monetisation. The analysis result identified seven partnerships worth considering in any organisation, as follows: The first partner is the data source owners,

who can add value to the organisation by providing essential data for a meaningful report for the business stakeholders. Thus, this partnership should follow a sustained data-providing strategy. The second partner is the client, who can support the decision makers to overcome the concerns and problems associated with customer requirements in case the requirement is unclear. The third partner is hardware and software vendors, who provide the required hardware and software capabilities and know-how of the technical factors of the new technologies, as they will reduce the risk of implementing such technologies and provide their expert feedback. The fourth partner is the crowd, or the ability to compete in the market and be internally and externally innovative. This can be accomplished by offering the data scientist the chance to meet innovation needs and overcome the existing challenges. The fifth partners are industry, governmental, and regulatory bodies, as data monetisation aims to manage the ongoing changes in different industries. Thus, powerful and effective policies and regulations are required in order to serve the market in all aspects. The sixth partner is academia, which can support data monetisation in two ways: 1) by developing a new approach and algorithm techniques that organisations can obtain on their existing capabilities and 2) academic entities also can build a great marketplace skill. Finally, the seventh partners are competitors and other peer organisations, when the two or more competitors work together in order to obtain the most benefits from the collected data, as in the case of advertisements in websites where buyers (advertisers) and sellers (media entities) can collaborate to gain a win-win revenue model through advertisements and easily reach their target market.

Furthermore, Tallon, Wixom & Buff (2015) found that there are two common themes in the best practices of the seven addressed partnerships: transparency and fairness. Transparency is the ability and willingness of the partner to understand the partnership sharing, limitations and market controls (Tallon, Wixom & Buff 2015). Moreover, fairness is based on

the fair-trade approach through fair benefits exchange among the industry (Tallon, Wixom & Buff 2015).

2.1.4 Strategic Pathway

As stated by Najjar & Kettinger (2013), data monetisation should follow a strategic pathway; it is essential to evaluate the technical (data structure) and analytical/logical (employee) skills of the organisation to determine the best data monetisation strategic pathway to follow (Najjar & Kettinger 2013). Technical skill is the organisation's ability to operate the hardware, software and network to collect, store and retrieve data (Najjar & Kettinger 2013). In addition, logical skills are the mathematical capabilities and logical business knowledge of the organisation's employees (Najjar & Kettinger 2013). The organisation that has data analysis and know-how skills will be at an advantage to process data and compete in the big data industry.

However, Najjar & Kettinger (2013) indicated that if the organisation's technical and logical capabilities are low, they will have three different pathways to follow in order to obtain high capability skills. The first pathway is moving directly to high risk and high reward; this way is very risky for data monetisation as it demands intensive technical and logical skills. Thus, a large investment is required to reach the target quality and capabilities for data monetisation. The second pathway is to first construct the logical capability; it mainly manages to train employees or hire candidates who have the skills required for data monetisation. It focuses on building in-house skills; thus, an internal investment is required to reach the target. The third pathway is to first construct the technical data infrastructure, which focuses on building an effective platform to share data efficiently and securely. The platform can be built in-house or with the support of the service provider to be hosted as a cloud infrastructure to control and speed up the platform creation. Additionally, this platform expedites the data

monetisation process and cuts analytical skills costs, which can be provided directly from the platform rather than building in-house. This path leads the organisation to reach the target quickly as it depends on outsourcing capabilities.

2.1.5 Strategy Themes

Romualdo-Suzuki (2015) developed a strategy structure that follows six themes: 1) Developing the city's data market by assessing, planning, and developing its centre of data innovation and making the city a store for data innovation, 2) Organising city data for impact by creating a fully mapped valued picture, offering well-documented APIs, and carrying out the existing metadata schema, 3) Recognising the value of city data by launching a range of valued cases for data extraction from public and private sources engaged with existing publishers of city data, 4) Building public acceptance by working with personal data and a trust network, creating a consumer data council and investigating the privacy aspects and support calls, 5) Active and effective governance by strengthening governance across city data by establishing a city data board and setting up a city data exchange to encourage all the partners to set their requirements, and finally, 6) The technology road map by providing a secure data exchanging environment and powerful platform to handle Internet of Things (IoT) data as well as constructing architecture that fulfils an end-to-end set of functional and non-functional requirements for the public sector.

2.1.6 Frame Data Monetisation Strategy

Data Monetisation is when the potential value of data is extracted and a profit achieved from it, usually through data trading (Najjar & Kettinger 2013). Data may also be monetised by transforming it into further tangible benefits (e.g., supplier funded advertising and discounts) or by avoiding costs (e.g., IT costs) (Najjar & Kettinger 2013).

Four critical discovery concepts to framing data monetisation strategy are highlighted by KPMG (2015). First is the Aggregation concept, collecting different types of data and creating a more centralised observable frame that includes data with aspects of more dimensions. Second is the Triangulation concept, in which different datasets are combined and new insights found. Additionally, data is validated with more than one cross-validation source. Third is the Frame of Reference concept, figuring out different insights from different angles and perspectives of the stored data. Fourth is the Privacy Preservation concept, following a balanced risk control and value protection approach (KPMG 2015).

2.1.6.1 Challenges

The main foundation for a valuable data monetisation strategy is highlighting the data sources and categorising them based on their impact on each organisational sector (KPMG 2015). However, there are some technological challenges that need to be addressed in order to achieve successful data monetisation (KPMG 2015). First is data overload; the vast amount of data is one of the challenges of data monetisation. Thus, some organisations plan to have new infrastructure to handle it. Second is data access; it is rare to have formatted data that can be easily gathered and used. Third is data cleaning – the more data is organised and qualified, the more the outcome insights there will be. Hence, data cleaning is very critical; it is very challenging to obtain cleaned data from different data sources. Fourth is data scalability; the process of high dimensions and complex data collection is very essential and critical, alongside aspects such as collection, storage, consuming and delivery to end users. However, the framed monetisation strategy should overcome the technological challenges to gain strategy goals and keep in mind that the data monetisation strategy is a business initiative and not an IT project (KPMG 2015).

Najjar & Kettinger (2013) addressed some challenges of collaborating with suppliers in monetising data strategy. Export data to suppliers can exclude the competitive advantage that could be achieved through asymmetric[1] information (Najjar & Kettinger 2013). All stakeholders should agree on a contract of mutual benefits agreement. Trust, privacy, and security should be addressed to overcome the risks. The data package should be clear in order to identify the required revealed data and the appropriate shared format and price (Najjar & Kettinger 2013). Pricing and marketing models should be considered.

The main challenge for each company is to figure out the relationship between data analysis and developing new products. Each organisation has multiple use cases through data analysis (Wilberg et al. 2017). Thus, the challenge is to spot an effective use case that delivers the expected value. Hence, companies should understand their target and objective of data monetisation. After finalising the scope, companies could proceed with data collection and analysis (Wilberg et al. 2017). It is also essential to have different levels of strategies that identify the direction of the company's vision (Wilberg et al. 2017).

2.1.6.2 Success Factors

Success factors are measured through; 1) institutional capability, meaning how successful the knowledge integration is in data infrastructure to obtain an outcome with knowledge cooperation and innovation, 2) social capability, which indicates the effectiveness of data participation and strategy support to develop the community in addition to educational sectors and R&D, and 3) innovation capability or outcome impact gathered from the conducted experiments and open innovation (Romualdo-Suzuki 2015). The key success of data monetisation is through partnering, which gives the organisation an opportunity to gain the

[1] Asymmetric information is when one of the partners has additional information and takes the control.

necessary resources and capabilities for the data monetisation process (Tallon, Wixom & Buff 2015).

2.1.6.2.1 **Non-Technical Factors**

Some non-technical factors need to be addressed. For instance, 1) In an enrichment road map, it is important to keep the data and analyses updated and find aspects to enhance the strategy. 2) Capture and dissemination economics means to consider all the costs related to the monetisation process and make sure to gain the predicted value from the consumed data cost. 3) Network effect and natural barriers are when an entity relies on third-party sales or delivery to get work with data and analyse or predict the organisation business flow. It will be difficult for the clients as they will switch to another provider; thus, this network will create a natural barrier. 4) Asset determination and financing implications figure out the potential output and opportunities from all aspects to monetise and obtain revenue. 5) Partnerships and organisation structure are essential to increase the outcome values (KPMG 2015).

2.1.6.3 Integration

The main aspects to be considered on a data monetisation platform are integration in order to gather data from different sources and integrity to make sure that such data is appropriate to support the monetisation process (Information Builders 2018). In fact, research in Aberdeen proved that an organisation without data quality solutions has about 22% massive faults on their records (Information Builders 2018). The final aspect is to provide analytics by providing different access to the involved participants for better interaction through, for example, dashboards and mobile BI (Information Builders 2018).

2.1.6.4 Managers Skills

According to an interview conducted on the critical change strategy over the next three years, Hertzfeld (2017) highlighted the required skills for revenue managers. Of the people

interviewed, 86% indicated that analytical or critical thinking is important (Hertzfeld 2017). However, 70% indicated that business expertise and strategic analysis skills ranked as the second important skills for revenue managers (Hertzfeld 2017).

2.2 Data Monetisation Business Models

The four common monetisation business models as addressed by KPMG (2015) are: the Return On Advantage Model, which means to use an organisation's internal collected data with other demographic information to create more added value for the organisation, such as targeting customers, risk mitigation and fraud recognition. Second, the Premium Service Model provides services to end-users through portal access with a monthly/annual subscription fee. Third, the Differentiator Model indicates building the organisation's loyalty brand by providing extra services to loyal customers without additional fees. Finally, the Syndication Model aims to provide data to third parties to develop their own analysis and reports for their internal advantages.

Data monetisation requires a business unit focused on building technical and business capabilities for the scope of a data monetisation strategy (Woerner & Wixom 2015). This focused business unit supports governing the data monetisation elements that differentiate one organisation from another (Woerner & Wixom 2015). Data monetisation can be conducted through three processes: selling, bartering and wrapping (Woerner & Wixom 2015). Selling is when a company sells an information-based product and gets their money back (Woerner & Wixom 2015). Bartering is when a company trades off its existing services to get new services or tools to enhance the current process and offered product (Woerner & Wixom 2015). Wrapping is when a company wraps its data with other core services and products and makes it more attractive to customers (Woerner & Wixom 2015).

2.2.1 Date Monetisation Procedures

According to Information Builders (2018), four main data monetisation procedures are required to be addressed as follows: 1) Need to know what is the most valuable information to be delivered to customers either internally or externally. Thus, organisations should focus on one or two pieces of information that have a valuable impact on generating revenue or reducing costs (Information Builders 2018). For example, the Yellow Pages acknowledged that the Return on Investment (ROI) has an effect on advisors to provide enhanced customer interaction by being able to view their digital marketing campaigns through an effective application (Information Builders 2018). 2) Need to know the data sources and plan for them by gathering the treasured data and consolidating them (Information Builders 2018). For instance, Scotiabank gathered all its data from more than 1000 branches to provide new ways to gain revenue and reach customers easily. Consequently, Scotiabank expected $250 million in annual sales throughout all the offered products (Information Builders 2018). 3) Need to figure out if the collected data is ready to be monetised by maintaining the most qualitative data and removing all the redundancies that create a wall in front of the monetisation process (Information Builders 2018). For example, global information management company Informa has a solution that cartelises and structures the people's contact information and saves it in a unique database that helps many countries. This central client profile platform has enhanced customers' satisfaction and upsold the organisation's revenue (Information Builders 2018). 4) Need to know about the required stakeholders who should be involved in such a data monetisation strategy. An organisation should only consider participants who can implement the agreed data strategy and give them the required access to achieve the assumed goal and have an impact on data monetisation (Information Builders 2018). For example, Pennsylvania-based organisations increased their revenue by letting the business and clinical users analyse the health records (Information Builders 2018).

2.2.2 Data Monetisation Impact

Woerner & Wixom (2015) addressed the effect of big data on building an organisation's business model. Big data helps to build data management by producing the following three new elements: new data, unique insight, and innovative action (Woerner & Wixom 2015). Accordingly, this implies receiving new data by inserting sensors to track the products and understanding customer behaviour and preferences through data feeds in social media (Woerner & Wixom 2015). Thus, with such new data, the organisation can examine unique and new insights by investigating the hidden analytics of the gathered data and viewing them in a powerful visualized software such as figuring out the products preferred by the customers. As a result of such dynamic insights, the organisation can decide and act accordingly by offering more from the preferred product and maintain the outcome quality.

2.2.3 Data Monetisation Outcome

There are two main approaches to monetise the collected data: using it to gain more revenue or saving the exiting costs (Information Builders 2018). Moreover, there are various ways to gain money through data monetisation, such as: selling the generated data, charging stakeholders for the outcome analytics of these data, maximising the loyalty of the existing customers through CRM, helping desk data, maximising customers' shares, understanding customers' needs and providing special personalised offers and services (Information Builders 2018). For instance, Helzberg Diamonds motivates their employees to retrieve insights from the point of sale (PoS) thereby resulting in 230 stores being examined to track the sales and performance among others (Information Builders 2018). In addition, the second approach, saving money using the data intelligence, would support controlling the spending costs and reduce them through the following: resource reallocation and inventory management to get rid of the wasted resources, inefficient operation removal, and expense reduction by assuring the product quality (Information Builders 2018). For example, the data monetisation purpose of

Quinte Health Care is to reduce $10 million from the operating budget, thus allowing managers to save money based on the data analytics in order to make a valuable decision (Information Builders 2018).

The data monetisation strategy provides two major monetising values. Firstly, performance value contributors aim to improve the existing performance of an organisation regarding an existing product through a benchmarking application that includes all factors of risk, growth, and efficiency suggestions (KPMG 2015). Secondly, predictive value contributors help gain predictive aspects that can feed another examined model for further qualitative decisions (KPMG 2015).

Moreover, commercial market and data monetisation usage should be focused on using the delivery focus concept that consists of three layers: 1) vertical value delivery, which involves providing valued data products or solutions to a specific industry; 2) horizontal value delivery, which provides similar solutions to different industries; 3) cross-market value delivery, where the gathered data value from one industry can be used and valuable to another industry (KPMG 2015).

2.2.4 Generating New Revenue

Generating new revenue streams using big data has a significant potential (Hertzfeld 2017). Producing revenue is a type of data monetisation – as introduced by the McKinsey Global Institute report on Big Data - which will generate more than $700 billion in terms of value to end users including both customers and business users[2]. Accordingly, the five key attributes to generate new income are as follows (Hertzfeld 2017) :

[2] https://www.ibmbigdatahub.com/blog/5-key-attributes-effective-data-monetization-strategy Accessed on 15 November 2018

1. Identifying the target customer needs, requirements, and goals by investigating their behaviours and customer surroundings.
2. Identifying data assets from all types of ‘raw, refined from both internal and external’ data, since monetisation is about generating revenue through the outcome insight from data enablers in order to differentiate between organisations.
3. Addressing regulatory and legal issues with technology in terms of overcoming the highlighted risks and introducing innovative policies that meet the regulatory and legal requirements as well as maintain customers’ trust.
4. Offering data as a service and business model, where data monetisation is targeted for the right business model and best strategic alliance and collaboration with the right partners, thereby aiming to achieve a win-win model to provide the best insights for customers as well as extended customers.
5. Defining the technology strategy, such as Hadoop, Spark, and IBM Watson Data Platform, which are open-source technologies recommended for collaboration with new fresh data to provide a real-time analysis for easy data monetisation.

Furthermore, business intelligence is extremely crucial for predicting future trends to find the best revenue market (Hertzfeld 2017). According to the Hospitality Sales & Marketing Association International questioner about the critical change strategy over the next three years, the outcome included 40% of replies suggesting a move from revenue management to predictive analytics while almost 24.2 % replies chose full integration of revenue management with sales and marketing; further, 22% choose to consolidate revenue management with business strategy and only a few selected to align revenue management with IT (Hertzfeld 2017).

2.2.5 Emerging New Products/Services

Currently based on the investigation of Johnson, Friend & Lee (2017), data monetisation leads to new product/service development processes resulting in disruptive innovation, which starts from the source of data instead of the moderate market flow comprising three mechanisms: cost, accessibility, and the business model structure. For instance, Uber, 23andMe, and Netflix, where Uber used big data to change the transportation logistics market by offering cost-effective drivers and more accessible transportation services compared to taxi services (Johnson, Friend & Lee 2017). Moreover, 23andME used big data to change the method of developing drugs in pharmacies, which is a cheaper and more advanced structure (Johnson, Friend & Lee 2017). Finally, Netflix used big data to offer better content services to customers at a low price using an effective and scalable streaming platform better than the existing content platforms (Johnson, Friend & Lee 2017).

3 Chapter Three: Methodology

An effective and critical literature review is essential to highlight the basic and advanced knowledge of any research. Such review is significant to figure out the previous theory, unaddressed areas, and the existing gaps that need to be discovered (Granic & Marangunic 2015).

The procedure of this study is to present a systematic review of the recent studies that covers all aspects and domains related to personal data monetisation. In addition, an online survey was conducted to observe the UAE's awareness and knowledge of sharing and monetising personal data as a case study, which has been elaborated in Chapter Five.

This systematic review is conducted by following the published guidelines of performing a systematic review (Al-emran, Mezhuyev & Kamaludin 2018). Furthermore, this study conducted a systematic review constructed on the following steps: recognizing data sources and search schemes, identifying the inclusion and exclusion criteria, conducting quality assessment, and data coding and analysis (Al-emran et al. 2018). More details of these steps have been explained in the following sub-sections.

3.1 Data sources and search strategies

The selected researches involved in this systematic review were collected from the vast published studies available in March 2019 within the following search engines: Google Scholar and journals databases such as Emerald Insight, IEEE, and Science Direct. Moreover, the search terminologies contain the following keywords, as demonstrated in Table 1.

Keyword Search
‘Identity Personal Data Monetization Strategy’
‘Identity Personal Data Monetization’
‘Personal Data Monetization’
‘Personal Data’ AND ‘Data Monetization’
‘Data Monetization’
‘Personal Data’

Table 1: Keywords Search
(Created by the Author)

The total studies on these keywords included 6,004,521 articles. As presented in Figure 1, the collected studies from Google Scholar, Emerald Insight, IEEE, and Science Direct were 4,982,500, 434, 22,903 and 998,684 articles, respectively.

The paper selection procedure in this study varied due to the large number of articles from each database and search engine. Therefore, only the relevant studies were selected based on personal data monetisation and following the search keywords as shown in Table 2.

In this systematic review, 17,500 papers were reviewed in Google Scholar and only 46 relevant studies were selected. Similarly, 437 papers were reviewed in Emerald Insight and 67 papers were selected. Additionally, after a review of 1,900 publications in IEEE, 60 papers were selected. Finally, 59 papers were selected after reviewing 600 papers from Science Direct. Hence, a total of 20,437 papers were reviewed and 232 articles were retrieved to be considered and assessed, as presented in Table 2.

Database	Reviewed papers	Selected papers
Google Scholar	17,500	46
Emerald Insight	437	67
IEEE	1,900	60
Science Direct	600	59
Total	**20,437**	**232**

Table 2: The Number of Reviewed and Selected Papers
(Created by the Author)

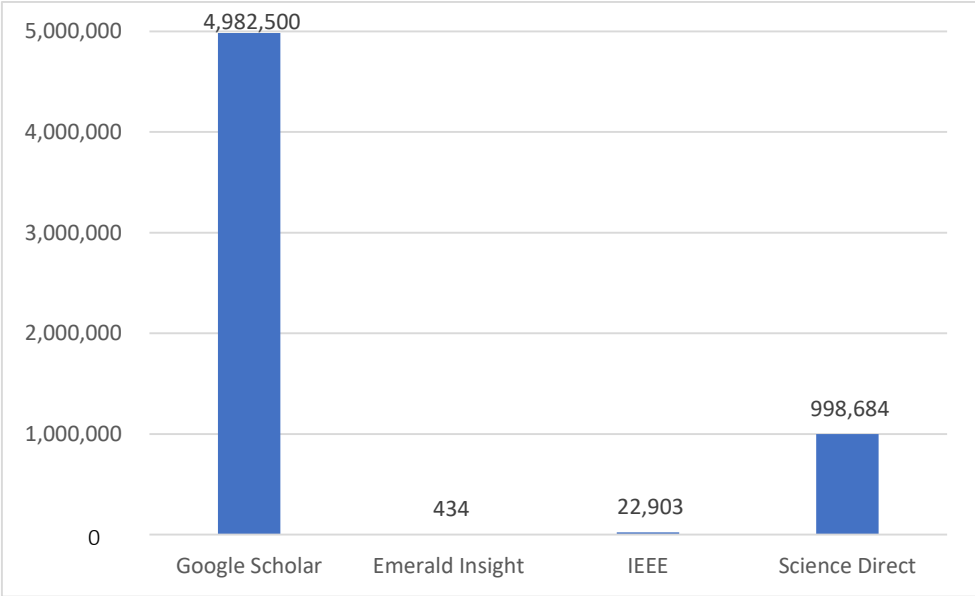


Figure 1: Total Studies on Identity Personal Data Monetisation Strategy in Each Database
(Created by the Author)

3.2 Inclusion and Exclusion Criteria

The nominated articles published in journals and conferences were selected based on the inclusion and exclusion criteria explained in Table 3. Moreover, there were 182 filtered studies after applying the inclusion and exclusion criteria as per the systematic review process illustrated in Figure 2.

Inclusion Criteria	Exclusion Criteria
The article should have been published not earlier than 2002	The article is not written in English
Any publication before 2014 must be very relevant and add value to be added to the topic	The article is published before 2014 with less than 10 citations and will not add any value to the topic
The article should address personal data monetisation	The article addresses data monetisation but not personal data monetisation
The article preferred must be cited by minimum 10 and above papers	The article does not address the research questions
The journal rating is recommended to be A ranked	The article is incomplete
The journal's impact factor should be 0.5 and above	

Table 3: Inclusion and Exclusion Criteria of Personal Data Monetisation Researches
(Created by the Author)

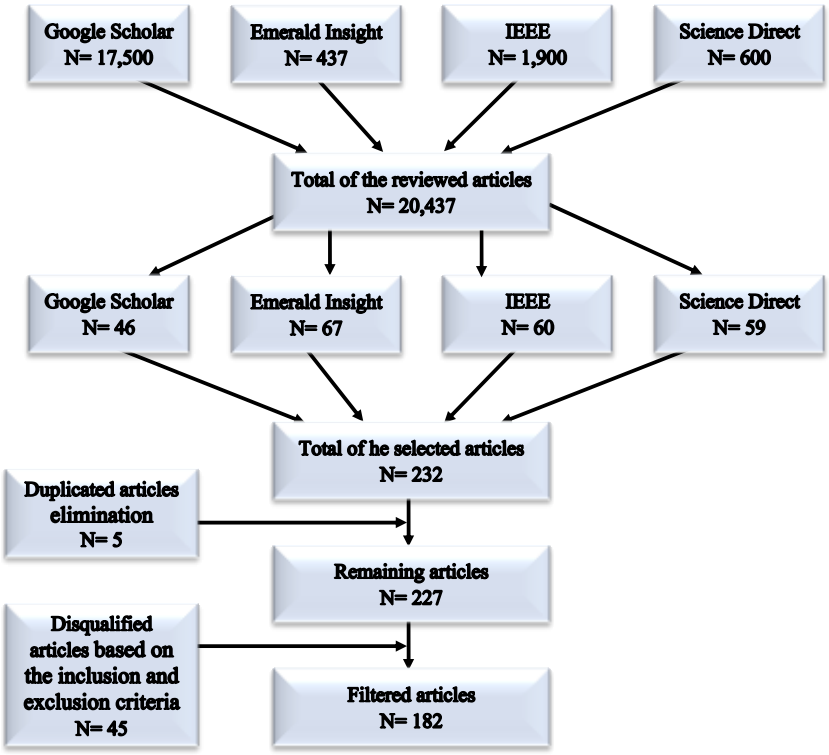


Figure 2: Systematic Review Process
(Created by the Author)

3.3 Quality Assessment

The quality assessment is an essential step alongside the inclusion and exclusion criteria. Moreover, the quality assessment checklist is considered with 10 criteria, which are applied on the 182 filtered articles. The quality assessment checklist criteria have been presented in Table 4. Further, this assessment checklist is not proposed as a method of criticism of any researchers' effort (Kitchenham & Charters 2007).

No.	Quality Assessment Questions
1	Is the aim of personal data monetisation clearly identified?
2	Is the problem of personal data monetisation clearly stated?
3	Does the study mention a clear challenge of the personal data monetisation?
4	Does the research discuss the affected factors of personal data monetisation?
5	Does the study highlight the related work of personal data monetisation?
6	Does the article mention the used methodology to monetise personal data?
7	Does the study explore the outcome according to personal data monetisation?
8	Are the supported countries of personal data monetisation clearly highlighted?
9	Is the personal data monetisation context clearly specified?
10	Does the study discuss the customer's concerns while monetising their personal data?

Table 4: Quality Assessment Checklist Criteria
(Created by the Author)

The scoring evaluation is inspired by Al-emran, Mezhuyev & Kamaludin (2018). Accordingly, each inclusion criteria will be scored with a three-point scale as follows: ‘yes and relevant to the related question’ worth 1 point, ‘no and not relevant to the related question’ worth 0 points and ‘partially and might be relevant to the related question’ worth 0.5 point. Hence, each study will be scored from 0 to 10. Consequently, the higher scoring study indicates its relevance to address the related research questions and vice versa. Table 5 presents the scoring results of the 182 papers.

3.4 Data Coding and Analysis

The associated features of the study methodology quality of personal data monetisation have been coded as follows: (a) the corelated definitions; (b) the common aim; (c) the common problem; (d) the common challenges; (e) the main affected factors; (f) the major related work; (g) the common methodology; (h) the common outcome; (i) the supported countries; (j) the main context; and (k) the customer concerns. During the data analysis, any paper that didn’t highlight any personal data monetisation procedure or characteristics was excluded from this study. Therefore, each paper was analysed manually by the author of this study as presented in appendix A.

4 Chapter Four: Results and Discussion

As per the filtered 182 articles published on personal data monetisation from 2002 to 2019, this study has presented the systematic review results of the four research questions.

4.1 RQ1: What are the co-related definitions, common aims, problems, and challenges of the personal data monetisation process?

4.1.1 Results

4.1.1.1 The Co-Related Definitions of The Personal Data Monetisation

4.1.1.1.1 Personal Data (PD)

PD stands for any data associated with personal identification. Furthermore, identification information is any data and information that can identify the person directly or indirectly, which is specified by a certain identification number or other factors, such as their mental, cultural, social, physiological, physical, and economical identity (Aldhouse 2014; Mojžiš & Laclavík 2016; Skendzic, Kovacic & Tijan 2018). In simple terms, PD covers every activity that an individual performs online or in the real-world, including their behaviour, actions, habits, and preferences (Dong et al. 2017; Tago et al. 2018; Vescovi et al. 2015).

4.1.1.1.2 Personally Identifiable Information (PII)

PII is any piece of data and information that could possibly identify any individual. Furthermore, it is information that distinguishes one individual from another, which includes sensitive and insensitive data[3].

[3] https://searchfinancialsecurity.techtarget.com/definition/personally-identifiable-information Accessed on 18 May 2019

4.1.1.1.3 **Personal Information**

Any information related to the individual when they purchase, create, access, maintain, and use anything in their daily life activities is known as personal information (Osothongs & Sonehara 2014; Osothongs, Suppakitpaisarn & Sonehara 2015; Rousseaux & Saurel 2016; Sinn, Kim & Syn 2019). Moreover, personal information is separated into two categories: general information and sensitive information. General information includes email address, phone number, etc; sensitive information includes health records, religious or political data, etc. (Kamaruddin, Dix & Razak 2011).

4.1.1.1.4 **Personal Information Management**

It is any action or activity that an individual or an organisation perform according to personal information (Sinn, Kim & Syn 2019). These activities include handling, categorising, and retrieving data on a daily basis (Kamaruddin, Dix & Razak 2011; Vescovi et al. 2015).

4.1.1.1.5 **Personal Service Data**

Personal service data is rather a significant collection as it contains the full history of service usage for each person, including their preferences and behaviours while using such services (Zhao et al. 2014).

4.1.1.1.6 **Personal Informatics (PI) Technologies**

PI technology tools are means to improve self-monitoring management, track individuals' behaviours and visualize personal data from different contexts (Rapp & Cena 2016).

4.1.1.1.7 **Personal Data Store (PDS)**

PDS is a facility allowing users to gather, govern, and structure their sensitive personal data through an extremely secured technique (Vescovi et al. 2015; Chowdhury et al. 2018; Anciaux, Nguyen & Popa 2013; Hildebrandt, O'Hara & Waidner 2013).

4.1.1.1.8 **Personal Data Lake**

It is a unified storage platform developed with powerful facilities correlated to personal data collection, storage, analysis, and queries. Accordingly, the data will be collected, analysed, and managed to be ready for any query by the data consumer (Walker & Alrehamy 2015).

4.1.1.1.9 **Data Brokers**

Data brokers collect, analyse, and bundle huge piles of sensitive personal data, which they trade as a packaged product to each other as well as advertise to organisations and markets, usually without data providers' awareness and permission (Parra-Arnau 2018).

4.1.1.1.10 **The Data Monetisation Concept**

Data monetisation has multiple levels. It may refer to the process of converting a non-monetary form of data objects service to other enhanced services or a form of cash and money value (Adjei 2016).

4.1.1.2 The Common Aims of the Personal Data Monetisation Process

Most organisations are looking for the efficient trend of stored personal data in their databases. Below are the common aims of the personal data monetisation process that have been addressed in 89 selected articles from different domains.

4.1.1.2.1 **Observe Users' Behaviour**

Linton et al. (2019) stated that they monetised their users' mobile usage in order to gain knowledge of their behaviours on mobile devices and the services offered by the suppliers. Moreover, it helped in providing valuable insight into futuristic decisions from the industry experts. In addition, Rivera, Croes & Zhong (2016) used personal data to observe the significant elements of mobile applications that might indicate user preferences.

4.1.1.2.2 **Recommendations**

Several studies have discussed the purpose of monetising personal data from the organisations' perspective in order to offer the best recommendations for their customers (Sanchez-Reillo et al. 2017). For example Liljander et al. (2015) examined young customers and the brand recommendation aspects based on their behaviour interactions. Further, such recommendations will improve the users' experiences and provide targeted offers (Evens & Damme 2016) and personalised services (Kim & Kim 2018). For example, PersonalIzed web paGe rEcommendatiON (PIGEON) filters movie search data based on a topic-aware Markov model and presents a chart to show interesting topics themes for each subscriber as well as discover the interesting preference patterns (Mei et al. 2018).

4.1.1.2.3 **Security**

Exploring customers' awareness about the security policy was aligned with search engines, which controls their online decisions based on the provided personal data (Ghosh & Singh 2018; Gabisch & Milne 2014). In addition, the above involves investigating users' concerns about their data privacy (Lusoli & Compañó 2010; Kuehn 2013; Kelley & Bertenthal 2016; Baloyi & Kotze 2017a)

4.1.1.2.4 **Reshape the industry marketplace**

This is a data age, where each person has the power to reshape the industry demand based on their data. Moreover, this personal data has an economic value across different domains (Becker 2014; Galbreath 2002; Adjei 2016), such as revealing new business opportunities (Anciaux et al. 2019), innovating digital contents (Simon 2016; Cummins et al. 2014), developing efficient application services (Chen & Kao 2006), and impacting the transformation of critical areas (Fortin & Uncles 2011). Such monetisation procedures are essential to meet customer satisfaction and expectations (Frecè & Selzam 2017; Owusu-frimpong 2008), for example, in the hospitality industry (Kasavana, Nusair & Teodosic 2010), retail (Mark Lee 2016), the food market (Prentice, Chen & Wang 2019), telecommunication services (Smailovic, Galetic & Podobnik 2013), and the healthcare industry (Hopia et al. 2015; Kim & Choi 2019; Plastiras & O'Sullivan 2018), etc.

4.1.1.3 The Common Problems of the Personal Data Monetisation

The personal data monetisation procedure has some problems addressed in different studies. Below are the common problems of personal data monetisation that have been lectured in 45 selected articles from different domains.

4.1.1.3.1 **Data Providers Losing Control on their Personal Data**

As indicated by Hirsch (2019), based on the poll conducted by the Pew Research Centre, Tett (2018) acknowledged that 91% of Americans stated having lost control of their personal data. However, it is essential for data providers to know who controls their personal data on the internet (Gabisch & Milne 2014) and how they can access it (Kurtz et al. 2019). Furthermore, large datasets of personal data are controlled by different service providers instead of data providers (Zheng et al. 2018; Zyskind, Nathan & Pentland 2015). Moreover, data providers don't have any control on their personal data monetisation process, which is

conducted by data consumers (Adjei 2016; Norta, Hawthorne & Engel 2018). However, users don't have any authority to control their data. Additionally, Nakagawa, Matsuda & Ogi (2013) stated that there was a problem of the lack of a practical method of providing personal data to any service provider under the data providers' control.

4.1.1.3.2 **Lack of Privacy on the Provided Personal Data**

Currently, although many users get personalised offers and services, they lose their personal data privacy in return (Portilla 2018). Moreover, personal data security is extremely essential for both the data providers and data consumers. Furthermore, privacy concerns have increased due to frequent security disclosures (Choi, Lee & Sohn 2017). In fact, users have lost their privacy while receiving improved and enhanced personalised services and offers through personal data monetisation (Estrada-Jiménez et al. 2019).

4.1.1.3.2.1 The Healthcare and Tourism Sectors

In the healthcare sector, the data providers are the patients who provide very sensitive personal data. However, they lose their privacy and have to acquire data transparency from healthcare providers (Bolton et al. 2018). In addition, patients' personal data should be anonymised before being analysed or used for healthcare purposes (Lim et al. 2014). Furthermore, in the tourism sector, personal data leakage and illegal usage lead to privacy and risk concerns for data providers (Wang 2018).

4.1.1.3.2.2 Information Misuse

As indicated by Nguyen & Simkin (2017), data misuse occurs due to the lack of privacy. Moreover, sometimes, the focus is only on the monetisation of personal data instead of considering on the generated value of such data (Frecè & Selzam 2017). In fact, the available personal data piles up substantially, thereby resulting in exposure to multiple attacks, abuse, and disclosures (Beldad, De Jong & Steehouder 2011; Kolter, Netter & Pernul 2010; Mojžiš &

Laclavík 2016; Sanchez-Reillo et al. 2017). Further, sensitive data – such as biometric data – loses its value when converted to technical information, which leads conversion into ordinary data rather than valuable, sensitive data (Štitilis & Laurinaitis 2017). Thus, there should be more critical research focused on personal data protection similar to the research conducted in Indonesia by Gandhi, Sucahyo & Ruldeviyani (2019).

4.1.1.3.2.3 Lack of Privacy Laws

As per the study conducted by Baloyi & Kotze (2017a), on the readiness of personal data protection regulations in South Africa, the existence of personal data privacy laws don't mean much unless they are verified as being efficient in practice, based on effective mechanisms. For instance, there is an ongoing process to build effective legal protection of electronic commerce transactions (Han 2015).

4.1.1.3.3 **Personal Data Storage**

It is necessary to store personal data in a unified, centralised storage, which must be used professionally (Bataineh et al. 2016; Zhao et al. 2014; Zheng et al. 2018). However, personal information is a collection of different attributes. Therefore, it is challenging to reserve the full raw data of personal information at once (Zhong & Liu 2009). Furthermore, since data collection is captured in a dynamic manner, redundancy and mismatching data aspects should be considered (Guo & Ma 2017). Accordingly, some organisations use cloud-based data storage to collect high volume, velocity, and variety of data, such as the Wiki-Health cloud-based platform. However, several problems are aligned with managing such massive data (Li et al. 2014).

4.1.1.3.4 **Personal Data Trading**

There are some illegal untrustworthy data collectors, for example, an offered application asking for personal data for illegal trading. Accordingly, it is a lack of reasonable

personal data trading platforms (Osothongs & Sonehara 2014). Consequently, there should be a proper way for data providers to control and trade their personal data in an efficient manner (Nakagawa, Matsuda & Ogi 2013). In addition, data providers share their data without any monetary reward. Moreover, a platform classifying the data type, quality, demand, and monetary value based on the time change (Bataineh et al. 2016) is also unavailable.

4.1.1.3.5 Data Providers' Lack of Awareness about what is Done with their Personal Data

It is crucial to investigate if users are aware and care about monetising their personal data as well as the risks associated with their personal data during such monetising processes (Baloyi & Kotze 2017b). This monetisation procedure is done without the data provider's permission (Sangani 2010). As per the survey conducted by Baloyi & Kotze (2017b) illustrated in Figure 3, it was found that only 79.7% of the respondents were conscious of their personal data misuse risk, and 20.3% didn't know about the finance and identity related issues, among others regarding the exploitation of their personal data.

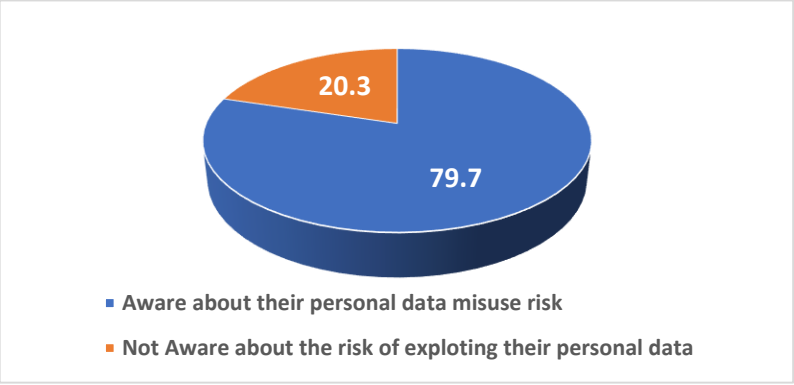


Figure 3: Percentage of Users' Awareness about Personal Data Risk
(Created by the Author)

In fact, individuals must be conscious of their personal data values (Malgieri & Custers 2018). Furthermore, while some parts of the personal data are not supposed to be monetised, others should be monetised appropriately (Malgieri 2018).

4.1.1.3.6 **The Exposure of Personal Data in IoT Networks**

Very little effort has been made to investigate the problem of disclosing personal data in IoT networks. Thus, users are concerned about their data from attacks that occurs due to unauthorised access. In addition, not much attention is paid to the prediction risks of users' behaviour conducted by third party applications, for example, tracking users and predicting their behaviour by sniffing wireless traffic (Torre, Adorni, et al. 2016).

4.1.1.4 The Common Challenge of the Personal Data Monetisation

The personal data monetisation practice has some challenges as lectured in the published researches. Below are the common challenges of personal data monetisation that have been addressed in 68 selected articles from different domains.

4.1.1.4.1 **The Challenge of Collecting and Storing Personal Data**

The main challenge is of personal data being stored in the cloud. Accordingly, the cloud infrastructure security should be exceptionally assessed since it acts as the cornerstone of digital evolution (Anciaux et al. 2019). In fact, these data are stored in several service clouds (Vianna et al. 2014; Zhao et al. 2014). However, data providers face a challenge in accessing their data (Tracol 2015; Zhong & Liu 2009). For instance, in the healthcare sector, patients face challenges when wanting to access their data in a unified system – which includes their full health history – while visiting multiple healthcare centres. Such access might be required for in-depth information and urgent data availability based on the patients' health status (Alsahafi & Gay 2018). Consequently, the vision of the Digital Health Revolution initiative will allow nations worldwide to access and control their personal data (Hopia et al. 2015).

Thus, data providers should ensure their data safety storage since they would be unable to have knowledge about how their data is being protected efficiently (Bae & Kim 2010).

Therefore, the new available technology should collect data and store them through different techniques that can't be misused (Bolton et al. 2018).

4.1.1.4.2 **Personal Data Protection Challenge**

Many users (data providers) mistrust the organisations that ask for their personal data unless they are assured of their privacy mechanisms (Katulic & Katulic 2018; Zyskind, Nathan & Pentland 2015). Moreover, based on the concept of hard privacy challenge, users don't trust data consumers to protect their personal data, as they only believe in their own methods of privacy protection and responsibility of their personal data (Anciaux, Nguyen & Popa 2013; Frey et al. 2017; Kirkham et al. 2013; Parra-Arnau 2018). Furthermore, although users refuse to offer data to the government and often provide wrong information – as they don't trust the government entities to secure their personal data – the risk of data sharing is expected (Beldad, De Jong & Steehouder 2011). In addition, the survey conducted in China by Wang & Yu (2015), found that females trust social organisations lesser than males, specifically in the social and personal network sector. Hence, this might decrease the users' motivations to reveal their data. However, it will result in limiting data availability for monetisation purposes (Dinero & Chua 2018; Gabisch & Milne 2014; Gerlach, Widjaja & Buxmann 2015). Furthermore, some users provide false information about themselves in order to protect their privacy, as stated by Murray-Rust et al. (2015).

Several personal data security breaches are reported daily, which are the outcome of inappropriate security methods leading to attacks from spoiled hackers (Feri, Giannetti & Jentzsch 2016; Jammalamadaka, Mehrotra & Venkatasubramanian 2011; Wang 2018; Zou 2016). Thus, data sharing has an extreme challenge requiring consideration characteristics such as data flexibility, scalability, frequency, and usability (Hernández-Ramos et al. 2018; Kong,

Wang & Zhang 2011). Therefore, Wu (2014) has addressed the national policy of protecting personal data and data protection laws (Baloyi & Kotze 2017a; García et al. 2018).

Moreover, Martínez et al. (2010) stated that there was an interest in protecting personal sensitive data in the healthcare sector through the identification of the best audit strategy and security measurement, similar to in the telecommunication sector (Moiso & Minerva 2012). Further, there is a challenge between the balance of data privacy and transparency (Mishra et al. 2015). Accordingly, patients should control sensitive shared data based on its sensitivity rank (Klein & Heines 2013) and provide it only to trusted healthcare providers (Francis & Francis 2017).

4.1.1.4.3 **Awareness of the personal data economic power challenge**

Data providers are unaware of their personal data's economic value. Further, they might underestimate their digital identity power (Baloyi & Kotze 2017b; Feijóo, Gómez-Barroso & Voigt 2014; Hildebrandt, O'Hara & Waidner 2013; Malgieri & Custers 2018). Thus, entities misuse and exploit such personal data for their own benefits and without users' permission and awareness of their data values (Faber et al. 2019; Malgieri & Custers 2018; Li 2017; Zharova & Elin 2017). However, data providers don't get any benefits and revenue, although the data is generated by themselves (Gerlach, Widjaja & Buxmann 2015; Nakagawa, Matsuda & Ogi 2013; Tudoran 2019), in addition to the lack of control or ownership on their data (Becker 2014; Lusoli & Compañó 2010). Besides, there is a challenge regarding pricing the information and personal data based on the data market (Adler, Stringer & Yap 2016; (Chessa & Loiseau 2017; Malgieri & Custers 2018). Moreover, if data providers are aware of their data price values, they can know their data's power in the market, thereby knowing how to safeguard their privacy (Malgieri & Custers 2018).

Users fear sharing their data as it might affect them as well as the data market negatively (Fred 2017; Schudy & Utikal 2017). Consequently, individuals must have the right to reveal or reserve their data in the data ecosystem (Vescovi et al. 2015). In addition, they should be conscious of the risk of revealing their personal data such as identity theft, financial fraud, etc. (Osothongs & Sonehara 2014; Torre, Adorni, et al. 2016). Currently, most available free applications generate their revenues based on in-app purchases, promotions, and mainly the collected usage data (Murray 2017). Additionally, sharing such data might reveal information about non-users' data (Choi, Jeon & Kim 2019). According to the survey conducted by Forum & Kearney (2014), 67% of the respondents indicated that many organisations ask for an extreme amount of personal data online (Dimakopoulos & Sudaric 2017). However, fewer than 40% of the respondents were confident and trusted online service providers such as online marketers, social media, etc. Hence, the former felt that sharing their data is risky and that these service providers are not trustworthy due to the lack of transparency between the users and data consumers (Oh et al. 2019).

Moreover, since the personal data outcome yields great revenue, data consumers use IoT devices in order to collect such data as much as possible (Oh et al. 2019). In addition, Personal Data Economy (PDE) challenges the data consumers' organisations in the consumer data market (Murray 2017). For example, there is a challenge while extracting the value that data providers put on their personal information, such as the difference between someone searching about a restaurant or about a fever drug. Further, users' online interaction can affect the financial outcome, as it depends on personal demographics such as education level, age, and gender, as well as other factors such as the location information (Carrascal et al. 2013). In addition, in the telecommunication sector, important data targeted for personal data monetisation are related to the users' habits, communication context as well as their favourites activities and interactions (Smailovic, Galetic & Podobnik 2013). Furthermore, media

companies should take users' trust into consideration in order to proceed with personal data capturing to provide personalised news and advertisements as well as to overcome their existing revenue challenges (Berman, Battino & Feldman 2011; Portilla 2018). The same should be applied in the hospitality sector (Linton et al. 2019).

4.1.2 Discussion

Personal data monetisation and data monetisation have multiple concepts and elements that have been identified along with their definitions in this question. This includes Personal Data (PD), Personally Identifiable Information (PII), Personal Information, Personal Information Management, Personal Service Data, Personal Informatics (PI) Technologies, Personal Data Store (PDS), Personal Data Lake, Data Brokers, and the Data Monetisation Concept.

There are several aims of the personal data monetisation process as shown in Figure 4. Accordingly, two studies are primarily focused on observing users' behaviour and tracking their daily activities, while five researches have focused on recommending the best and targeted personalised offers for each individual. In addition, 42 studies have discussed how to overcome security concerns and observe user awareness and 17 researches have observed the reshaping and enhancing of the industry marketplace. The above results are based on the selected addressed studies on each topic.

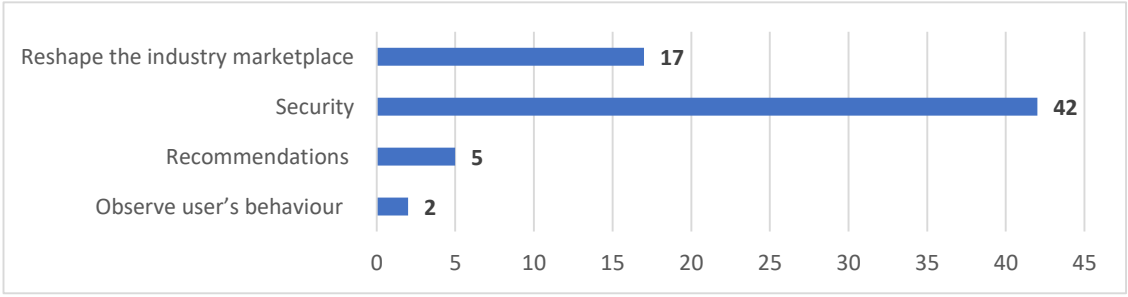


Figure 4: Number of Articles that Addressed each Personal Data Monetisation Aim
(Created by the Author)

In general, each process has certain problems. The same is with personal data monetisation process since it has problems related to the user data along with privacy, exploitation risk, and data ownership. As shown in Figure 5, several studies have addressed the following problems: losing data control, lack of data privacy and user awareness, data storage and trading issues, as well as data exposure in IoT networks. Moreover, scholars have mainly focused on the lack of privacy, which has been addressed in 16 researches, followed by the focus on losing control in nine researches, and an almost similar number of studies have discussed data storage, data trading, and lack of awareness in six, four, and five studies, respectively. Finally, one study has discussed data exposure in the IoT network

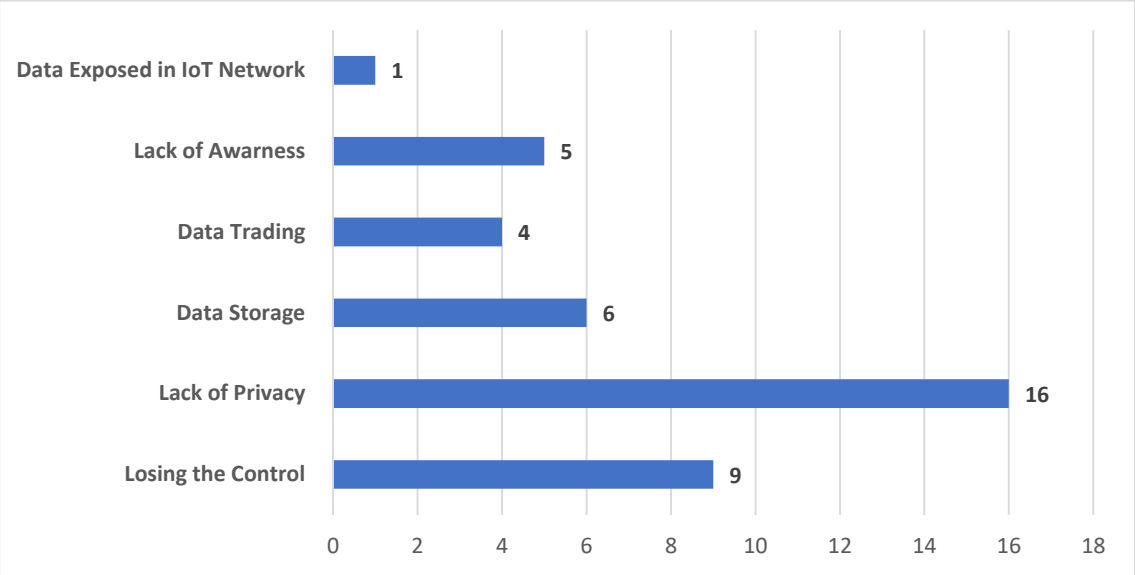


Figure 5: Number of Articles that Addressed each Personal Data Monetisation Problem
(Created by the Author)

There are several challenges associated with personal data monetisation, such as the data collection and storing procedures in an efficient and unified platform challenge. Further, the above involves the data protection challenge while safeguarding the users' safety and privacy, along with awareness about their data's economic value and power challenges. Figure 6 presents the number of researches addressing each challenge. Personal economic value awareness is clearly the significate challenge, with 33 addressed studies, and 26 studies on the

data protection challenge. Lastly, nine studies were conducted on data collection and storing challenges.

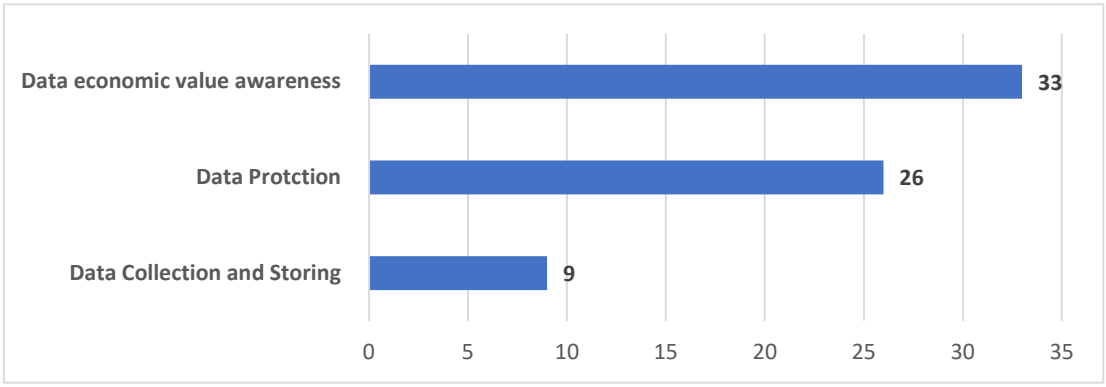


Figure 6: Number of Articles that Addressed each Personal Data Monetisation Challenge
(Created by the Author)

4.2 RQ2: What are the main factors that affect personal data monetisation along with the major related work and the common methodology used to monetise the personal data?

4.2.1 Results

4.2.1.1 The Main Factors that Affect Personal Data Monetisation

The personal data monetisation procedure has some influential factors that have been addressed in the published studies. Below are the common factors affecting personal data monetisation, which has been lectured in 13 selected articles from different domains.

4.2.1.1.1 Factors that Affect the User's Willingness to Share their Personal Data

As per the study conducted by Widjaja et al. (2019) confidence, suggested expense, and expected advantages are the key aspects that affect the clients' readiness to share their personal data (Dinero & Chua 2018). In addition, the connection and privacy interaction policy with service providers (Gerlach, Widjaja & Buxmann 2015; Kim & Choi 2019; Yavuz & Toker 2014) indicates that trust in each unit related to privacy is ranked in order as follows: 1) family; 2) healthcare; 3) scholars; 4) device manufacturers/application developers; 5) government

organisations; and 6) insurance entities. Moreover, the data collection procedure's creativity, expertise, and the tools intelligence applied by the service operators are affected as well (Kasavana, Nusair & Teodosic 2010).

The risk of data leakage is correlated to the ability of sharing personal data. For instance, the generated data of the IoT devices and the running applications of the device background leads to higher privacy risk concerns (Frecè & Selzam 2017; Kim et al. 2019; Torre, Adorni, et al. 2016). Moreover, the affected factors in this manner are mainly focused on the data collection procedure, management, and usage through the available resources (Guo & Ma 2017). Accordingly, Kim & Kim (2018) indicated that users were willing to provide their contact, biographical, and financial information. Therefore, overall, users were mostly willing to provide demographic and daily life information and unwilling to offer financial or personal identification information. Further, there is a strong willingness in the users' perspective about storing their sensitive data on the cloud at a cost in order to maintain their privacy and security concerns, compared to normal personal data, which is usually stored without any cost (Widjaja et al. 2019).

4.2.1.1.2 **Factors that Affect User Behaviour Tracking and Recommendation Services**

The technical, social, legal, and psychological factors affect user behaviour tracking and differentiate between what individuals say and do in reality (Carrascal et al. 2013). In addition, customisation service and recommendations depend on the readiness of the users to share their data (Bolton et al. 2018).

4.2.1.2 The Major Related Work of Personal Data Monetisation

The personal data monetisation procedure has several related works that have been lectured in the published researches. Below are the major related works related to personal data monetisation that have been addressed in 45 selected journal articles in different domains.

4.2.1.2.1 **The Existing Systems and Approaches**

As per the survey conducted to investigate the readiness of the personal information processing system, 42.9% of the participants developed personal information processing systems. In addition, management and technical people support such processing as a result of 44.44% and 41.38% respondents, respectively (Baloyi & Kotze 2017a).

4.2.1.2.1.1 Two-sided trading market

As stated by Bataineh et al. (2016), collecting data is not an easy task for both data consumers and providers. Therefore, from the data consumer's point of view, 1) they must find the right data provider to provide qualified data; 2) the data consumer often has limited financial plans for data acquisition; 3) they must choose a specific collection of data that meets their demands. In addition, data providers are required to 1) find data consumers who need their data; 2) have monetary knowledge about their data based on the market needs; and 3) increase their profit.

Thus, Bataineh et al. (2016) proposed a platform for personal data trading using the two-sided market concept. This trading platform deals with both data groups from consumers and providers to provide benefits for both sides. Consequently, such a platform highlights the purchasing price for data providers and selling price for data consumers.

For example, as highlighted in Table 5, the Datacoup platform permits people to generate cash from distributing their personal data (Parra-Arnau 2018) in addition to the CooPeD: Co-owned Personal Data management system and model (González-Manzano et al. 2014). Further, the ipShield platform helps users control what data to hide and share with others (Torre, Koceva, et al. 2016). Similarly, the Intelligent Personal Health Record (iPHR) was developed to provide more personalised healthcare services to patients in order to enhance their daily life activities (Kasuya et al. 2017). Moreover, Kolter, Netter & Pernul (2010) proposed a

visualisation platform that allows data providers to know and present their data records. In addition, Bae & Kim (2010) proposed Personal Information Protect (PIP), a model to secure data privacy by the individuals themselves without any interaction from the service provider (Choi, Jeon & Kim 2019). Further, the Data-Wallet management system allows for direct monetisation from personal data between the data providers and market consumers (Norta, Hawthorne & Engel 2018). Additionally, Smart-Pockets has the required techniques to allow the users to access their personal data and visualise them efficiently (Vatavu 2017).

Platform Name	Description
Datacoup	allows people to earn money while sharing their personal data
CooPeD	Co-owned Personal Data management system and model
ipShield	helps users control what data to hide and what data to share with others
iPHR	developed to provider more personalised healthcare services to patients in order to enhance their daily life activities
visualisation platform	allows data providers to know and present their data records
PIP	a model to secure data privacy by individuals themselves without any interaction from the service provider
Data-Wallet management	allows for direct monetisation from personal data between the data providers and market consumers
Smart-Pockets	has the required techniques to allow users to access their personal data and visualise them

Table 5: Two-sided Trading Market Platforms

(Created by the Author)

According to the survey conducted by Logicalis (2016), 42% respondents, more than a thousand UK citizens from 13 to 17 years old, prefer to earn money from their personal data rather than acquire salary from a job. In addition, as per the survey reported by Ponemon (2015) 56 percent of the respondents were willing to share their personal data as long as they received an economical reward. For example, users sell their data to get discount shopping coupons

(Dinero & Chua 2018; Feri, Giannetti & Jentzsch 2016; García et al. 2018; Malgieri & Custers 2018; Oh et al. 2019).

Furthermore, two-sided markets are found in many industries including credit card platforms; recruitment sites (job seekers and recruiters) such as Monster; search engines (advertisers and users) such as Google; Internet auctioneers (buyers and sellers) such as E-Bay; social networks (users and advertisers) such as Facebook and Twitter; video-game consoles (gamers and game developers) such as Sony; and yellow pages (advertisers and consumers) such as daily newspapers (Bataineh et al. 2016).

Dong et al. (2017) developed DSPM, a prototype aimed to improve the data discovery possibility. In addition, it allows the users to control their data in a way to maintain the data distributing and privacy security (Van Hoboken 2016) (Khovanskaya et al. 2013).

4.2.1.2.1.2 Personal data anonymisation

Data anonymisation techniques should be applied on all data elements as well as their environment. Moreover, anonymised information is not only about getting safe data, but useful data as well. Further, anonymisation reduces data-sharing risks. Thus, people can reveal their data to be used by other entities and to guarantee the confidentiality of the shared data through protection regulation as addressed by Elliot et al. (2018) and Scott (2013).

4.2.1.2.2 **The Existing Personal Data Protection Procedures**

4.2.1.2.2.1 Personal Data Protection Bodies

As presented in Table 6, currently, personal data protection follows the OECD guidelines to protect data privacy (Cha & Yeh 2018). However, there are several public personal data protection associations worldwide such as Federal Services for Technical and Export Control (FSTEC), Federal Services for Supervision of Communications, Information

Technology and Mass Communications and Federal Security Service (FSS) in the Russian Federation, which support personal data protection (Zharova & Elin 2017). Moreover, the European Union (EU) has the General Data Protection Regulation for personal data collection (Tikkinen-Piri, Rohunen & Markkula 2018), in addition to the governing model for personal data protection in social media applications in the United Kingdom (UK) (Haynes, Bawden & Robinson 2016). Similarly, the Malaysian government forced the personal data protection program through the Personal Data Protection Act (PDPA); however it had some issues as stated by Chua et al. (2017). Furthermore, a study conduct by Wu (2014) compared the major federal personal data protection laws in the e-government.

Supported Countries	Protection Bodies
36-member countries	OECD guidelines
Russian Federation	FSTEC
	Federal Services for Supervision of Communications
	Information Technology and Mass Communications
	FSS
EU	GDPR
UK	regulatory model for personal data protection in social media applications
Malaysian government	PDPA

Table 6: Personal Data Protection Bodies within the Supported Countries
(Created by the Author)

4.2.1.2.2.2 Personal Data Protection by Untrusted Entity

There are several data services available nowadays, such as Google Docs, Gmail, Outlook, and etc. Users usually use their personal data on such data services, which are called Web-based Data Services (WDSs). WDSs usually facilitate full data management and multiple web applications that help individuals to handle their personal data. There is a Data Protector

that acts as a middleman and controls the traffic flow between the browser and the web server (Jammalamadaka, Mehrotra & Venkatasubramanian 2011).

For instance, any developer in the Google ecosystem should agree on the Google Play Developer Distribution Agreement. In this agreement, there is a section which indicates that the developer will use any identification or personal data of the users. In that case, to protect the personal data, the developer should alert the users and obtain the legal privacy to protect their users (Fahy, Van Hoboken & Van Eijk 2018). If the trust relationship is betrayed it would have a negative impact on the monetisation process as well. Thus, the user's opinion of the trustworthiness of the Identity Management System (IdMS) is an essential factor in its accomplishment because users have a significant effect on the usage behaviour of the systems (Adjei 2014).

4.2.1.2.3 **Personal Data Value as a New Currency**

Dong et al. (2017) indicated that personal data is the new oil and the new currency of the digital world (Malgieri 2018; Moiso & Minerva 2012; Törngren 2017). There are some scholars investigating personal data value. Portilla (2018) and Otsuki & Sonehara (2013) indicate that the personal data value is estimated based on the cost of protecting the data.

This new currency is used by the recent huge data-driven associations, for example, Google, Twitter, and Facebook. These companies increase their earnings through personal data monetisation, either by selling the users' data, sharing them or tracking their users' behaviour through their searches and posts (Evens & Damme 2016; Carrascal et al. 2013).

Personal data means money. As stated by Shrier, Wu & Pentland (2016) there should be a new concept of treating personal data. There should be a personal data account similar to a bank account, which will enable the individual user to handle, supervise, deal with their data

in the same manner as they use with their personal bank account today (Nakagawa, Matsuda & Ogi 2013; Vishik, Svetlana & Suryanarayana 2011).

In addition, the personal data act as the critical revenue stream for each business activity. As per the conducted survey of around 600 organisations worldwide, 79% of them indicate that they collect data from their customers or service users, 42% from data sharing partnerships, 33% from the connected devices, and 33% from the third-party data suppliers. Organisations are looking for several alternatives to collecting personal data because the results benefit both data consumer and data providers. Such as 77% of the data consumers offer an enhanced user experience, 52% get in to the new market and 50% convert the products into much more innovative product or service (Cooper & LaSalle 2016). However, there are few academic works on estimating the personal information value (Feijóo, Gómez-Barroso & Voigt 2014).

4.2.1.3 The Common Methodology Used to Monetise Personal Data

The personal data monetisation process uses several methodologies that have been described in the following 54 selected journal articles in different domains.

Personal data monetisation processing systems are explored through several methodologies as shown in Figure 7. The major methodologies rely on surveys (53 percent) (Bradford, Earp & Williams 2017; Gerlach, Widjaja & Buxmann 2015; Hornik, Shaanan Satchi & Rachamim 2019; Kim 2017; Kim & Kim 2018; Kim et al. 2019; Linton et al. 2019; Tudoran 2019; Wang & Yu 2015; Widjaja et al. 2019), 16% relied on experimental designs (Gabisch & Milne 2014; Liljander et al. 2015; Rapp & Cena 2016) and case studies (Dann, Teubner & Weinhardt 2019; Martínez et al. 2010; Rivera, Croes & Zhong 2016), 10% relied on interviews (Ladhari & Tchetgna 2015; Rishi & Gaur 2012) and finally, 5% relied on focus group discussions (Adjei 2016).

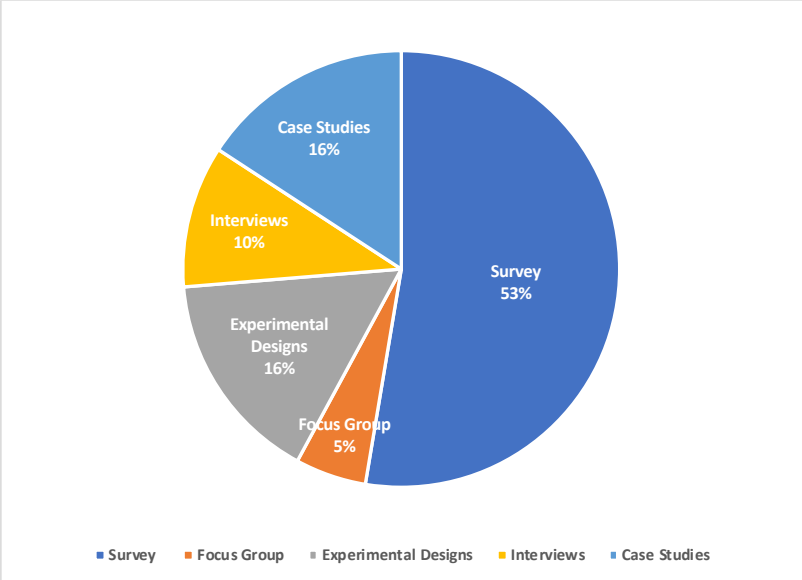


Figure 7: The Percentage of each Methodology in the Personal Data Monetisation Process

(Created by the Author)

Such methodologies are required in order to get more information of the essential elements for developing powerful models, tools, and frameworks as well as to observe the essential principles of maintaining the risk management policy, prevent data leakage and misuse, and protect the privacy of sensitive personal data privacy (Bae & Kim 2010; Cha & Yeh 2018; Gandhi, Sucahyo & Ruldeviyani 2019; Han 2015; Kong, Wang & Zhang 2011; Nakagawa, Matsuda & Ogi 2013; Torre, Adorni, et al. 2016; Vianna et al. 2014; Vinodhini & Ayyasamy 2017). In addition to providing control and ownership to the data provider through PDS, personal data trading platforms and two-sided market interact and engage in the data marketplace and receive the most valuable benefits (Anciaux et al. 2019; Anciaux, Nguyen & Popa 2013; Bataineh et al. 2016; Chessa & Loiseau 2017; Dong et al. 2017; Fortin & Uncles 2011; Hildebrandt, O'Hara & Waidner 2013; Kirkham et al. 2013; Kuehn 2013; Malgieri & Custers 2018; Oh et al. 2019; Osothongs & Sonehara 2014; Parra-Arnau 2018; Torre, Koceva, et al. 2016; Vescovi et al. 2015).

There are several systems and ways developed for collecting personal data, analysing them, and monetising them (Smailovic, Galetic & Podobnik 2013; Zhao et al. 2014). For the purpose of retrieving data, a trusted and secured approach provides the best-personalised services in today's digital world (Khovanskaya et al. 2013; Shrier, Wu & Pentland 2016). Multiple data brokers use blockchain to protect the collected data, specially the sensitive data, such as health records and identity management (Chowdhury et al. 2018; Faber et al. 2019; Zheng et al. 2018; Zyskind, Nathan & Pentland 2015) in addition to developing the tokenising ecosystem to maintain the privacy and anonymising such data (Elliot et al. 2018; Frecè & Selzam 2017; Kim, Lee & Lee 2019). For example, Zheng et al. (2018) proposed a crypto token named Personal Health Data coin (PHD coin), which is mined through gathering personal data on the blockchain-enabled ecosystem to accelerate the transactions.

4.2.2 Discussion

There are two influential factors in the personal data monetisation procedure. Firstly, the affecting factors of the user's willingness in order to share their data include trust and privacy maintenance. Secondly, the factors that affect their behaviour tracking and recommendation services are based on technical, legal, social, and psychological factors.

Moreover, there are several related works in the personal data monetisation process such as exploring the recent systems and approaches, which includes the two-sided trading market concept and personal data anonymisation. The existing personal data protection practices and the bodies in the different countries involved in data protection are shown in Table 7. The protection by untrusted entities is highlighted as well. Finally, the personal data value is a new trading currency and the percentage of the collected data from each provider entity is highlighted as well. Figure 8 illustrates the number of articles related to the personal data monetisation.

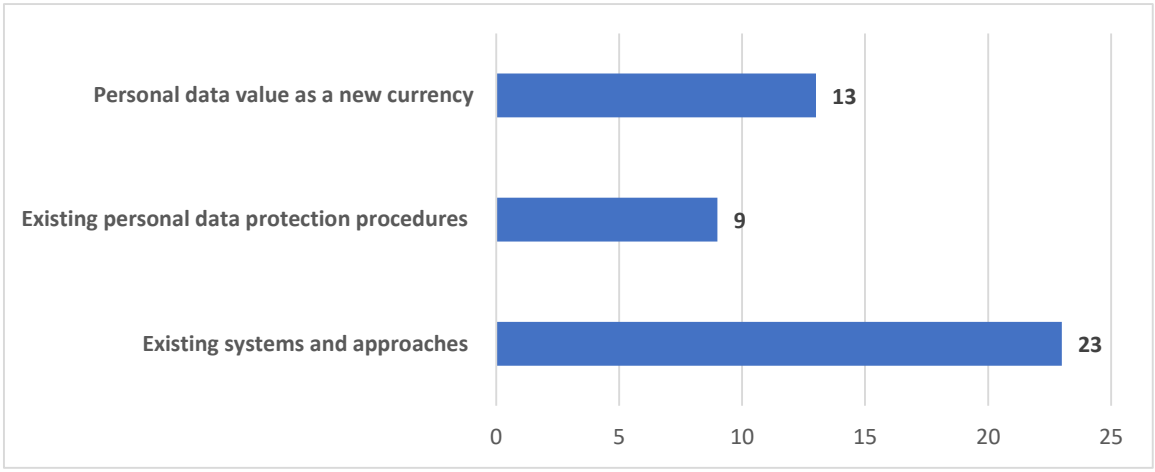


Figure 8: Number of Articles that Addressed each Personal Data Monetisation Related Work

(Created by the Author)

As may be noted from Figure 9, survey is the main method used by the researchers to explore the personal data monetisation process and evaluate its outcome efficiently. Many scholars investigated, developed, and tested the best algorithms and systems to monetise the personal data, get expected revenue, and provide personalised products/services in a secured approach.

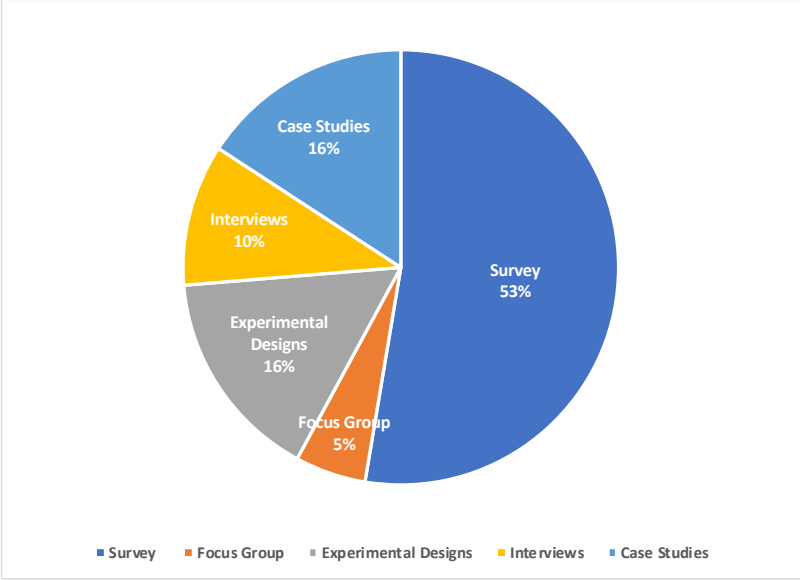


Figure 9: The Percentage of each Methodology in the Personal Data Monetisation Process

(Created by the Author)

Figure 10 shows the trendline of the number of methodologies used over the years. It is noticed that most of the methodologies in 2019 used the survey method. Also, from 2015 to

2018, the methodologies used for the personal data monetisation process decreased every year. However, it suddenly increased in 2019 and reached to six methodologies.

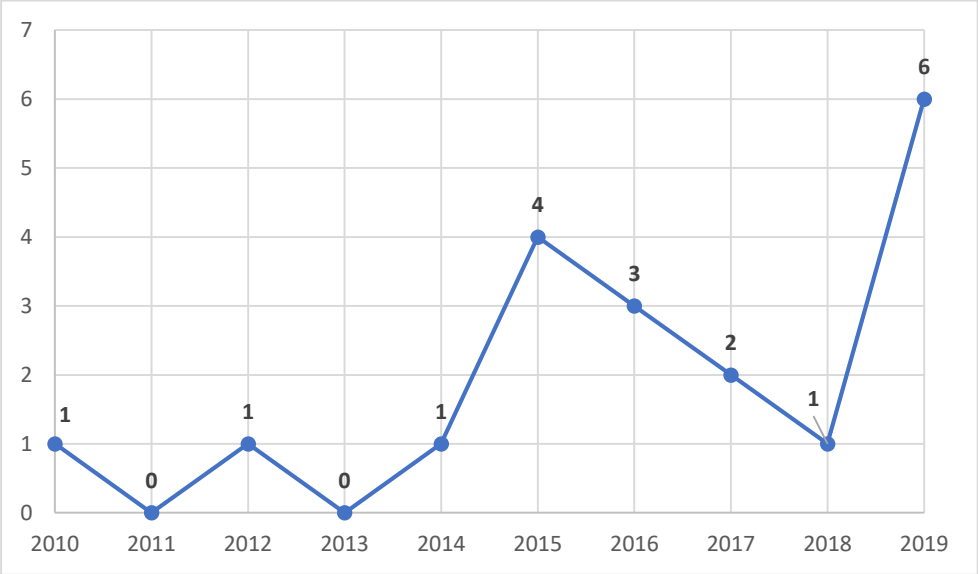


Figure 10: The Trend in the Number of Articles by Using Different Methodologies for Personal Data Monetisation Throughout the Years
(Created by the Author)

4.3 RQ3: What are The Common Outcomes of The Personal Data Monetisation, as well as The Main Contexts in which Personal Data Monetisation is used and the supported Countries of Personal Data Monetisation?

4.3.1 Results

4.3.1.1 The Common Outcomes of Personal Data Monetisation

The personal data monetisation procedure generated several outcomes that have been described in the published researches. Given below are the major outcome results which are related to personal data monetisation that have been addressed in 68 selected journal articles in different domains.

4.3.1.1.1 **Track Users' Activity to Provider Personalised Services and Offers**

Tracking users and monitoring their online activities is one of the major outcomes of the personal data monetisation process (Baloyi & Kotze 2017a; Grodzinsky, Gumbus & Lilley 2013). Such tracking leads to exploring the user's behaviour, preferences, and their lifestyles to provide efficient personalised services based on the agreement with the data providers (Adjei 2016; Bae & Kim 2010; Guo & Ma 2017). Each data received by the service users is an input for building and developing a personalised service or product (Chen & Kao 2006; Foster 2016; Norta, Hawthorne & Engel 2018; Scott 2013). For example, there are some persons who share their mobility data and personal experience to track the traffic directions, share location with relatives, and monitor their kids' activities (Baloyi & Kotze 2017b; Dinero & Chua 2018).

In addition, the users' preferences that are collected are distributed to trusted third parties to better target their advertisements and improve their users' experience (Carrascal et al. 2013; Cha & Yeh 2018; Choi, Jeon & Kim 2019; Dimakopoulos & Sudaric 2017; Estrada-Jiménez et al. 2019; Fahy, Van Hoboken & Van Eijk 2018; Kuehn 2013; Moiso & Minerva 2012; Törngren 2017; Tudoran 2019; Osothongs & Sonehara 2014). For instance, Facebook monetise their users' data through tracking and tracing data from the browsing cookies and sharing the data based on the user's history of preferences with advertisement agencies, which is called Re-Targeting (Smailovic, Galetic & Podobnik 2013). Also, such sharing supports the user organisations' management to make significant decisions to meet their users' preferences (Bolton et al. 2018; Moiso & Minerva 2012; Serrano, Greenhill & Graham 2015) and to target the most protentional customers (Han 2015; Kim et al. 2019). It enables the respective entities to provide much more accurate customised services and recommendations, such as for movies, restaurants, travel, music, news, and shopping (Berman, Battino & Feldman 2011; Chipp & Chakravorty 2016; Evens & Damme 2016; Kim & Kim 2018; Liljander et al. 2015; Linton et al. 2019; Mei et al. 2018; Oh et al. 2019; Portilla 2018; Rivera, Croes & Zhong 2016; Wu &

Gereffi 2018; Zhao et al. 2014), and develop new personal applications to enhance individuals' lives (Moiso & Minerva 2012; Vescovi et al. 2015), like healthcare prediction (Torre, Adorni, et al. 2016), genomics, and personalised medicine (Elmisery, Rho & Botvich 2015; Hopia et al. 2015; Mishra et al. 2015; Tikkinen-Piri, Rohunen & Markkula 2018).

4.3.1.1.2 **Driving Economic and Innovation Growth**

Personal data monetisation and the use of personal data which acts as the exchange currency in the new digital world, will lead to building modern business models and an innovative society (Adjei 2016; Cooper & LaSalle 2016; Moiso & Minerva 2012; Shrier, Wu & Pentland 2016). In addition, it will innovate a new channel for target marketing the right consumer by learning their online habits (Galbreath 2002; Spiekermann et al. 2015; Tikkinen-Piri, Rohunen & Markkula 2018; Wang 2018) and optimise decision making procedures and the prediction of future trends for increasing revenues (Hirsch 2019; Rivera, Croes & Zhong 2016; Zyskind, Nathan & Pentland 2015), for instance, developing personalised online gaming in the future (Barsky 2018) to generate revenue through advertisements, and in-app purchases at customised prices (Chessa & Loiseau 2017; Margarida Barreto 2013; Murray 2017; Ravoniarison & Benito 2019).

Some organisations indicate that there is no value to be derived from sensitive personal data. However, this does not exclude the business potential of getting each individual's valuable information (Lusoli & Compañó 2010), for instance, earning revenue from advertising through personal data monetisation (Gabisch & Milne 2014) and improving the existing services communication and reputation (Nguyen & Simkin 2017). Also, only personal data can be used multiple times without losing its value as long as it is used efficiently and in the right way (Feijóo, Gómez-Barroso & Voigt 2014; Spiekermann et al. 2015).

4.3.1.2 The Main Context in which Personal Data Monetisation is used

Personal data monetisation is conducted in multiple contexts. Figure 11 shows 79 studies that applied personal data monetisation in 17 different contexts.

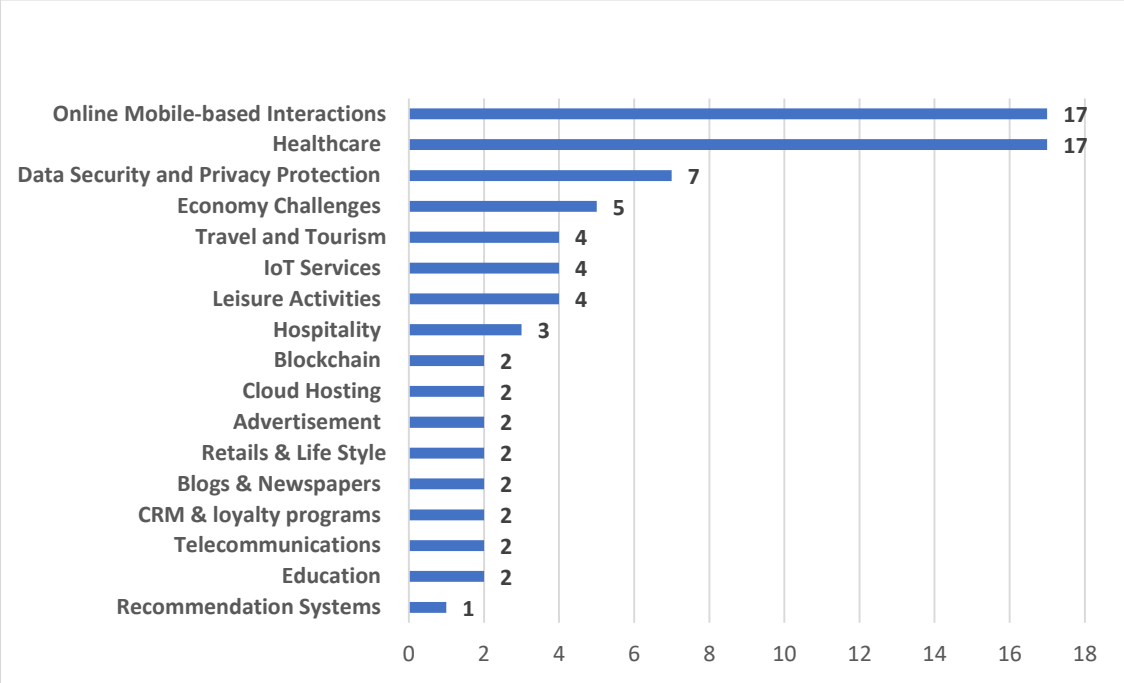


Figure 11: Number of Articles that Addressed each Personal Data Monetisation Context

(Created by the Author)

There are 17 studies that investigated personal data monetisation in the context of online mobile-based interactions, e-commerce, e-government, and social media (Beldad, De Jong & Steehouder 2011; Dinero & Chua 2018; Fahy, Van Hoboken & Van Eijk 2018; Gabisch & Milne 2014; Ghosh & Singh 2018; Guo & Ma 2017; Han 2015; Haynes, Bawden & Robinson 2016; Kim & Kim 2018; Moiso & Minerva 2012; Portilla 2018; Ravoniarison & Benito 2019; Tudoran 2019; Vishik, Svetlana & Suryanarayana 2011; Wu 2014; Wu & Gereffi 2018; Zajc 2015) and in the context of healthcare (Alsahafi & Gay 2018; Bolton et al. 2018; Elmisery, Rho & Botvich 2015; Fortin & Uncles 2011; Geissbuhler et al. 2013; Hopia et al. 2015; Karampela, Ouhbi & Isomursu 2018; Kim & Choi 2019; Klein & Heines 2013; Li et al. 2014; Lim et al. 2014; Lusoli & Compañó 2010; Martínez et al. 2010; Plastiras & O'Sullivan 2018; Regidor 2004; Wood et al. 2019; Zheng et al. 2018).

There are seven studies on data security and privacy protection (Anciaux et al. 2019; Choi, Lee & Sohn 2017; Parra-Arnau 2018; Štitilis & Laurinaitis 2017; Vatavu 2017; Wang & Yu 2015; Zharova & Elin 2017) and five studies each that explored economic challenges (Adjei 2016; Cooper & LaSalle 2016; Feijóo, Gómez-Barroso & Voigt 2014; Foster 2016; Kurtz et al. 2019).

Also, there are four studies that explored travel and tourism (Wang 2018; Linton et al. 2019; Rivera, Croes & Zhong 2016; (Lusoli & Compañó 2010) and leisure activities such as games and music (Berman, Battino & Feldman 2011; Fahy, Van Hoboken & Van Eijk 2018; Lusoli & Compañó 2010; Ravoniarison & Benito 2019) and on IoT services (Kim et al. 2019; Oh et al. 2019; Torre, Koceva, et al. 2016). There are three studies on hospitality (Kasavana, Nusair & Teodosic 2010; Rishi & Gaur 2012; Rivera, Croes & Zhong 2016).

Furthermore, there are two studies each on education (Lusoli & Compañó 2010; Sinn, Kim & Syn 2019), telecommunications (Smailovic, Galetic & Podobnik 2013), CRM & loyalty programs (Baird & Parasnis 2011; Nguyen & Simkin 2017), blogs & newspapers (Evens & Damme 2016; Liljander et al. 2015), retails & life style (Kasuya et al. 2017; Mark Lee 2016), advertisement (Estrada-Jiménez et al. 2019; Kuehn 2013), cloud hosting (Adjei 2014; Zhao et al. 2014), and blockchain (Chowdhury et al. 2018; Zyskind, Nathan & Pentland 2015). There is a single article that investigated personal data monetisation in the context of recommendation systems (Linton et al. 2019).

4.3.1.3 The Supported Countries of Personal Data Monetisation

There are several countries that led the development of personal data monetisation procedures due to their valuable outcomes and business growth. As presented in Figure 12, there are 11 pieces of research in the European Union, which discussed the personal data monetisation process and its challenges (Feri, Giannetti & Jentzsch 2016; Han 2015; Haynes,

Bawden & Robinson 2016; Mojžiš & Laclavík 2016; Osothongs, Suppakitpaisarn & Sonehara 2015; Portilla 2018; Sánchez-Cabrero et al. 2018; Štitilis & Laurinaitis 2017; Tikkinen-Piri, Rohunen & Markkula 2018; Tracol 2015; Wu 2014) as well as seven research endeavours in the United States (Brier 2017; Elliot et al. 2018; Feri, Giannetti & Jentzsch 2016; Han 2015; Kim 2017; Scott 2013; Wu 2014), and five studies from China (Han 2015; Prentice, Chen & Wang 2019; Wang & Yu 2015; Wu 2014; Zou 2016). In addition, there are two researches from Canada (Ladhari & Tchetgna 2015; Osothongs, Suppakitpaisarn & Sonehara 2015), Indonesia (Gandhi, Sucahyo & Ruldeviyani 2019; Widjaja et al. 2019), Korea (Kim & Choi 2019; Kim & Kim 2018) and Taiwan (Cha & Yeh 2018; Widjaja et al. 2019). There is one research each from Japan (Nakagawa, Matsuda & Ogi 2013), Malaysia (Chua et al. 2017), South Africa (Baloyi & Kotze 2017b), and Thailand (Osothongs, Suppakitpaisarn & Sonehara 2015). However, there are two studies that investigate personal data monetisation in small islands and other countries (Baloyi & Kotze 2017a; Rivera, Croes & Zhong 2016).

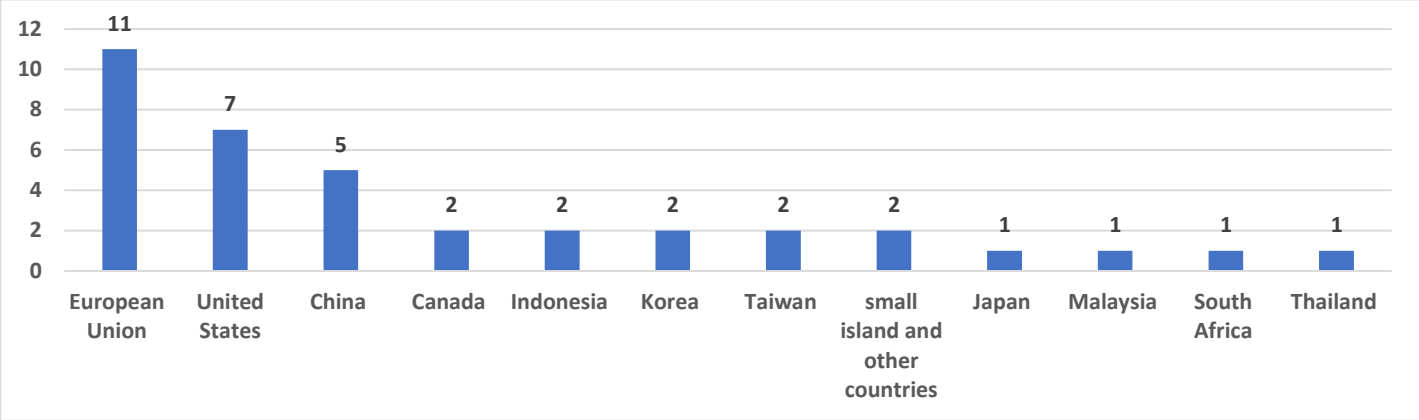


Figure 12: Countries that Support Personal Data Monetisation
(Created by the Author)

4.3.2 Discussion

The main outcome from the personal data monetisation process is the offer of the best personalised products and services. This can be done through tracking users' real life and online activities. In addition, users might get monetary value by revealing their data, which will increase the organisation's revenue and benefit the data providers as well. Moreover, such a process will drive for new economic development and innovative growth. Figure 13 shows the articles that addressed each monetisation outcomes. There are 21 articles on economic growth through personal data monetisation and 47 studies on tracking user's behaviour to propose the best personalised services and products.

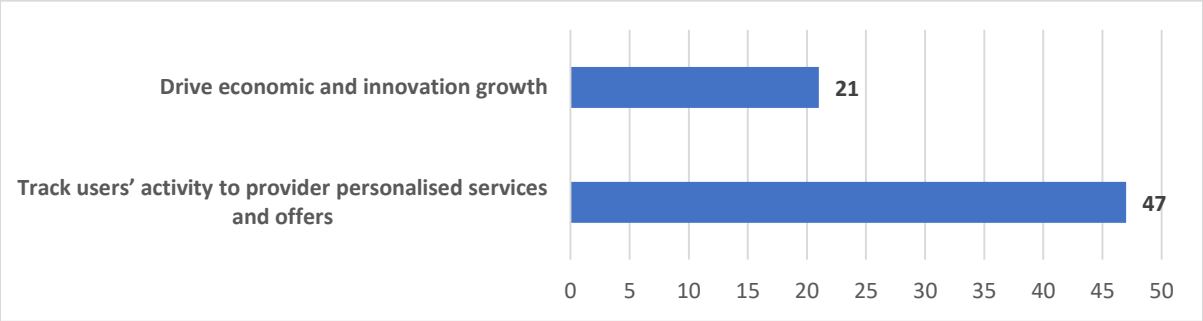


Figure 13:Number of Articles that Addressed each Personal Data Monetisation Outcome

(Created by the Author)

Each study addressed a specific context as mentioned above. Some researchers investigated the full contexts in their entirety while others did it partially, highlighting some of the features within the domain. Online interactions and healthcare emerge as the domains that evinced the greatest interest in the data monetisation process. These were followed by data security and privacy protection, economic challenges and travel and tourism. However, there is very little investigation into recommendation systems, which are distinct from the recommendation adds-ons that have an efficient outcome in the online applications.

The above mentioned studies highlight only the countries that implement personal data monetisation and show their willingness to use the procedure. However, only a few scholars

investigated the reflected outcome for each country, the positive and negative effects of the process on the citizens, and the economics of the industry in each country.

4.4 RQ4: What are the customer's main concerns about monetising their personal data?

4.4.1 Results

Scholars have highlighted 101 studies on the customer's main concerns regarding the monetisation of their personal data. The customers' main concern is over data privacy, protection techniques, and classifying the methods and approaches to sharing and transacting their personal data in a secure manner. Thus, the key elements for each customer or service user while sharing their personal data are the trust and confidence they have in the service provider, control and ownership of the personal data, and privacy protection (Adjei 2014; Adjei 2016; Anciaux et al. 2019; Anciaux, Nguyen & Popa 2013; Bae & Kim 2010; Baloyi & Kotze 2017a; Baloyi & Kotze 2017b; Bataineh et al. 2016; Becker 2014; Beldad, De Jong & Steehouder 2011; Biliri et al. 2018; Bolton et al. 2018; Brier 2017; Carrascal et al. 2013; Cha & Yeh 2018; Choi, Jeon & Kim 2019; Chowdhury et al. 2018; Chua et al. 2017; Cooper & LaSalle 2016; Cummins et al. 2014; Dann, Teubner & Weinhardt 2019; Dimakopoulos & Sudaric 2017; Dinero & Chua 2018; Dong et al. 2017; Elliot et al. 2018; Elmisery, Rho & Botvich 2015; Estrada-Jiménez et al. 2019; Fahy, Van Hoboken & Van Eijk 2018; Faber et al. 2019; Feri, Giannetti & Jentzsch 2016; Foster 2016; Francis & Francis 2017; Frecè & Selzam 2017; Fred 2017; Frey et al. 2017; Gabisch & Milne 2014; Galbreath 2002; Gandhi, Sucahyo & Ruldeviyani 2019; García et al. 2018; Geissbuhler et al. 2013; Gerlach, Widjaja & Buxmann 2015; Grodzinsky, Gumbus & Lilley 2013; Guo & Ma 2017; Han 2015; Haynes, Bawden & Robinson 2016; Hildebrandt, O'Hara & Waidner 2013; Hirsch 2019; Jammalamadaka, Mehrotra & Venkatasubramanian 2011; Kabanov 2016; Karampela, Ouhbi & Isomursu 2018; Kelley & Bertenthal 2016; Kennedy & Laczniak 2016; Kim et al. 2019; Kim & Kim 2018;

Kirkham et al. 2013; Kolter, Netter & Pernul 2010; Kong, Wang & Zhang 2011; Kuehn 2013; Kurtz et al. 2019; Li 2017; Li et al. 2014; Linton et al. 2019; Lusoli & Compañó 2010; Mark Lee 2016; Martínez et al. 2010; Moiso & Minerva 2012; Murray 2017; Nakagawa, Matsuda & Ogi 2013; Nguyen & Simkin 2017; Norta, Hawthorne & Engel 2018; Oh et al. 2019; Osothongs & Sonehara 2014; Osothongs, Suppakitpaisarn & Sonehara 2015; Owusu-frimpong 2008; Schudy & Utikal 2017; Štitilis & Laurinaitis 2017; Portilla 2018; Rousseaux & Saurel 2016; Sanchez-Reillo et al. 2017; Sangani 2010; Shrier, Wu & Pentland 2016; Tikkinen-Piri, Rohunen & Markkula 2018; Törngren 2017; Torre, Adorni, et al. 2016; Torre, Koceva, et al. 2016; Tudoran 2019; Van Hoboken 2016; Vescovi et al. 2015; Walker & Alrehamy 2015; Wang 2018; Wang & Tang 2012; Wang & Yu 2015; Widjaja et al. 2019; Wu & Gereffi 2018; Xiong 2015; Zou 2016; Zhihan, Quan & Lu 2016; Zharova & Elin 2017; Zyskind, Nathan & Pentland 2015).

4.4.2 Discussion

Figure 14 illustrates the trendline by the number of articles that addressed the customer's concerns every year from 2003 to 2019. The figure shows that the number of articles that addressed the customers' main concerns appeared in 2018, though scholars began to address customers' concerns in 2010. However, in 2012, the number dropped to three from five in 2011. Nevertheless, the number has risen sharply from year to year by 16% from 2013 to 2018. This increment indicates the increasing realization of the importance of customers' concerns over sharing their personal data.

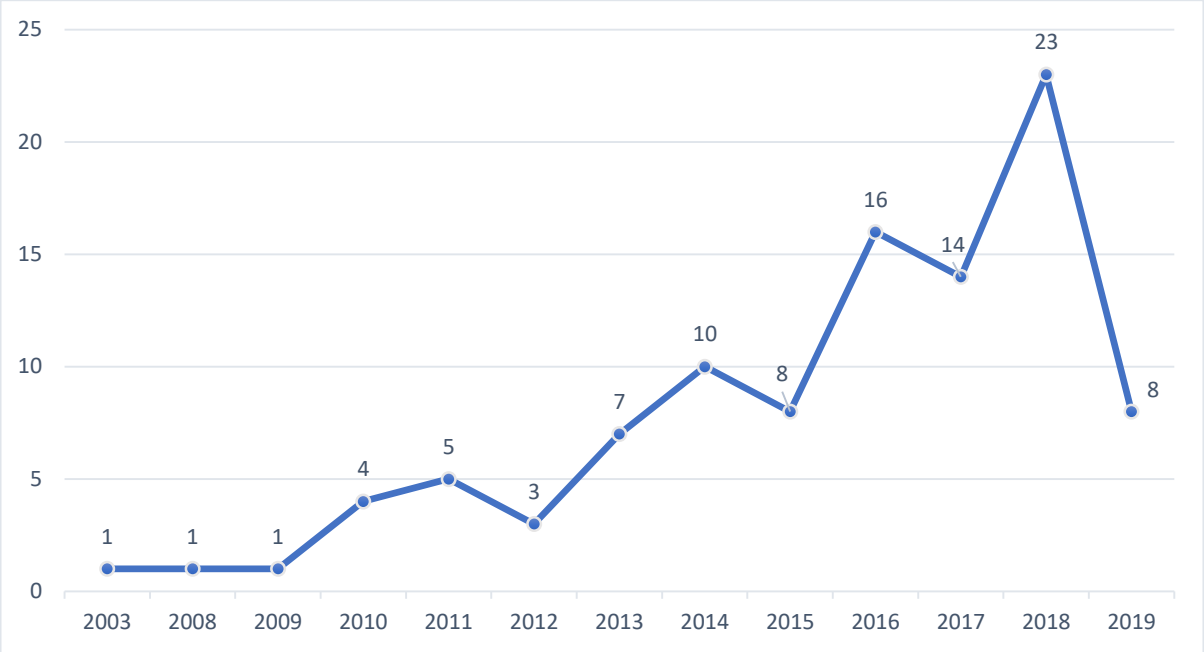


Figure 14: Numbers Showing the Trend in Articles that Addressed Customers' Concerns over Personal Data Monetisation Throughout the Years
(Created by the Author)

5 Chapter Five: UAE Case Study

The previous sections explored features of personal data monetisation and its aspects, privacy risk, and monetisation challenges. In the course of this study, a survey to investigate the UAE citizens' knowledge and awareness of their data sharing monetisation and usage was conducted. Given below are the findings from the survey and their resulting discussion.

The survey was prepared using an online link and sent to a randomly selected sample of the UAE citizens using various channels, namely, Instagram, WhatsApp, emails, Snapchat, Twitter, etc. Ethical guidelines were followed for the primary research which was prepared by Halej (2017). It was read and confirmed by the respondent, as a mandatory requirement, before initiating the survey. The responses from the participants in the survey were filtered, classified, and analysed.

5.1.1 Demographics Data

This survey was taken by 225 respondents of which 67.6% were female and 32.4% were males as shown in Figure 15. Those who were younger than 18 years and older than 55 years formed 1.3% each of the respondents, 18–24 year olds formed 43.1% of respondents, 25–34 year olds, 35–44 years, and 45–54 years old formed, respectively, 31.6%, 18.2%, and 4.4% of the total number of respondents as presented in Figure 16.

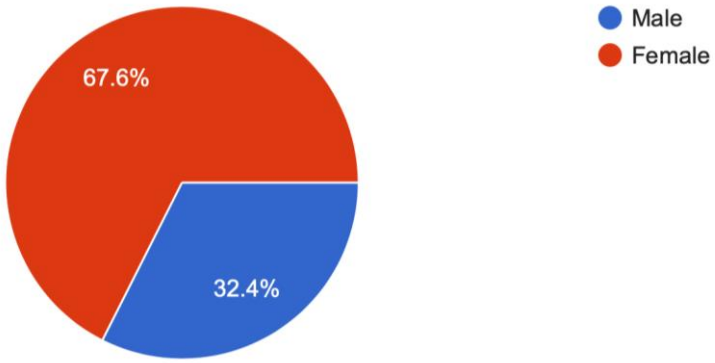


Figure 15: Gender Distribution of Survey Respondents
(Created by the Author)

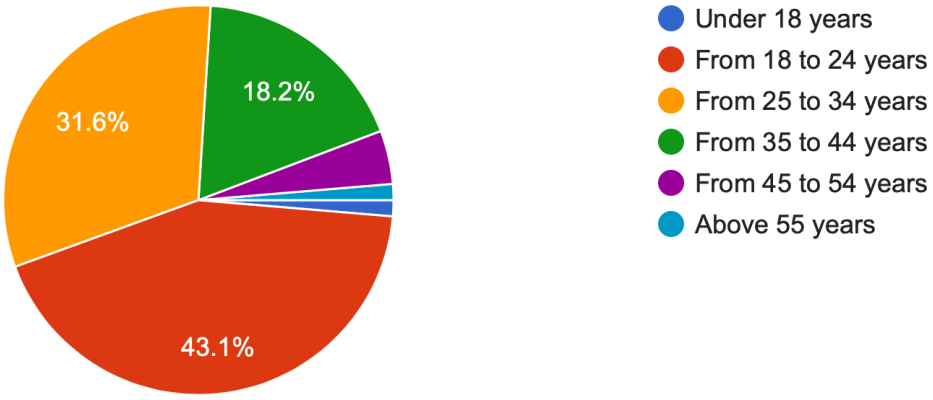


Figure 16: Age Category Distribution of Survey Respondents
(Created by the Author)

More demographics data of the respondents is presented in figures 17 and 18. Figure 17 shows the distribution of respondents according to their educational qualification. Most of the respondents are bachelor's degree holders at 60%, 12% studied up to high school, 8.4% were high school graduates, diploma, or the equivalent. A master's degree was held by as few as 18.2%. Only a few held a doctoral degree.

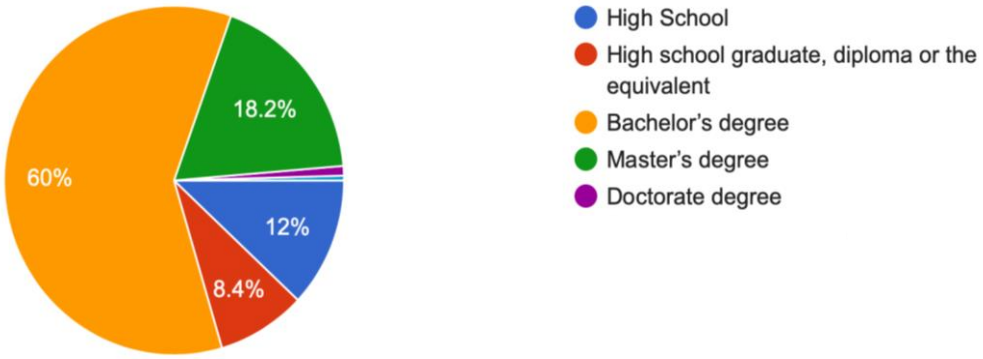


Figure 17: Distribution of Survey Respondents According to Highest Educational Qualification as in 2019
(Created by the Author)

Also, figure 18 shows the employment status of each respondent. About 57 of the respondents were employed, 23.6% were students, and 12% were unemployed. Also, the self-employed and housewife categories form 3.1% and 2.2% of the population, respectively. Those retired from work and unable to work formed 1.7% of the respondents.

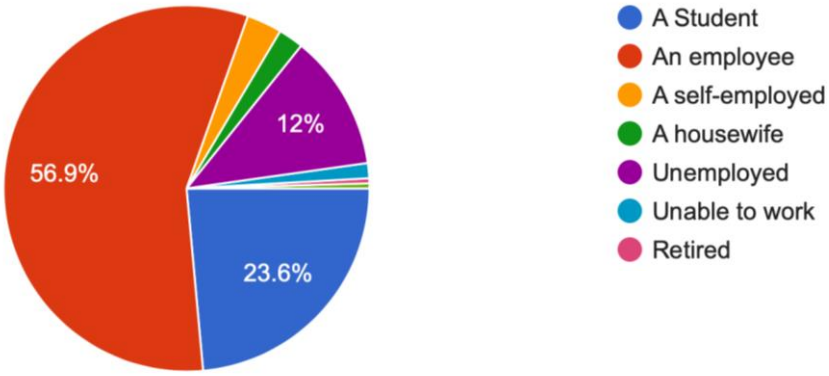


Figure 18: The Employment Status Distribution of Survey Respondents
(Created by the Author)

The respondents' break-up according to nationalities is presented in Figure 20. Most of the respondents are Emiratis. Also, seven respondents are from Jordan, five each from Pakistan, India, and Egypt, three each from Yemen and Comoros, and two respondents each were Sudanese, Lebanese, and Bahraini and one each from Serbia, Syria, Somalia, Tunisia, Palestine, Iraq, Kenya, France, Germany, Filipin, Czech Republic, Canada, Belize, and the USA. Of these, 95.6% of the respondents live in the UAE, as shown in Figure 19.

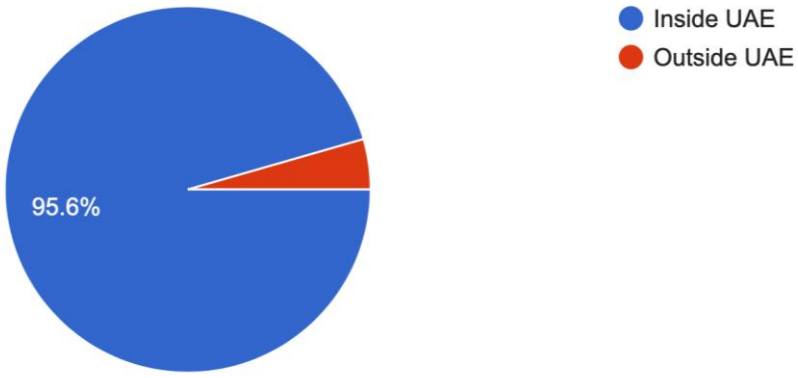


Figure 19: Percentage of the Respondents Who Live in the UAE
(Created by the Author)

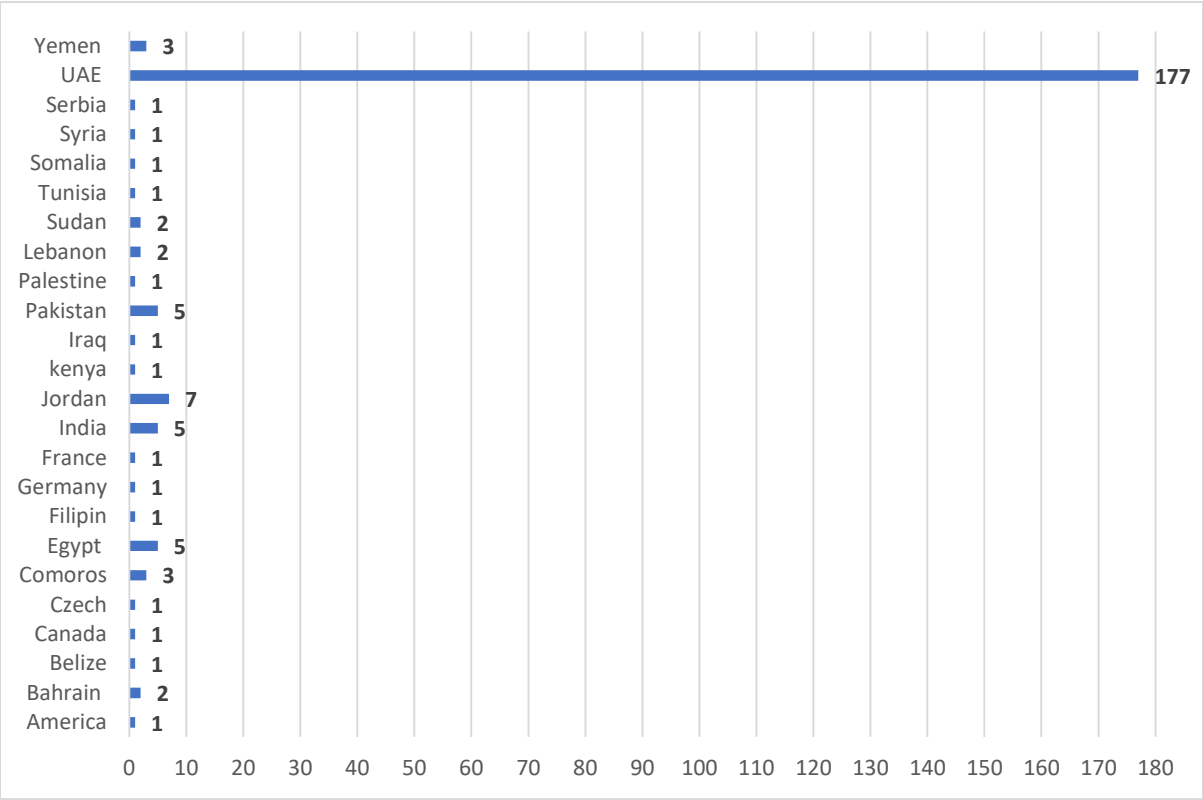


Figure 20: Distribution of Survey Respondents by Nationality
(Created by the Author)

5.1.2 Research Questionnaire Results

Of the 255 respondents, 37.8% confirmed that they had shared their personal data with others, 40.9% indicated that they did not share their personal data with anyone, and 21.3% were not sure if they shared their personal data or not as illustrated in Figure 21.

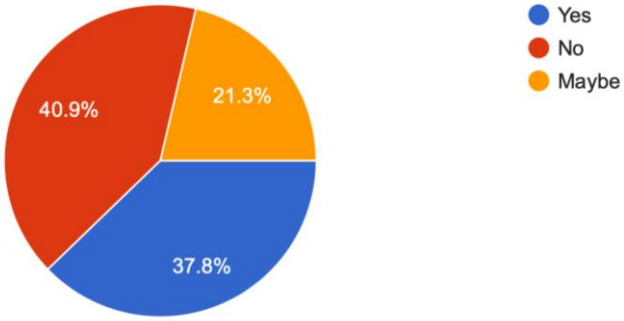


Figure 21: Percentages of Respondents who Shared or Did Not Share their Personal Data with Others
(Created by the Author)

The respondents who shared their personal data have mentioned the data types of their shared personal data. The shared data are Names, Phone Numbers, Emails, Addresses, and the required information required for registration in social media accounts, events, shopping websites, and other authorised entities. Also, bank account details, confidential passwords, date of birth and family information, and other data were shared. See Figure 22.

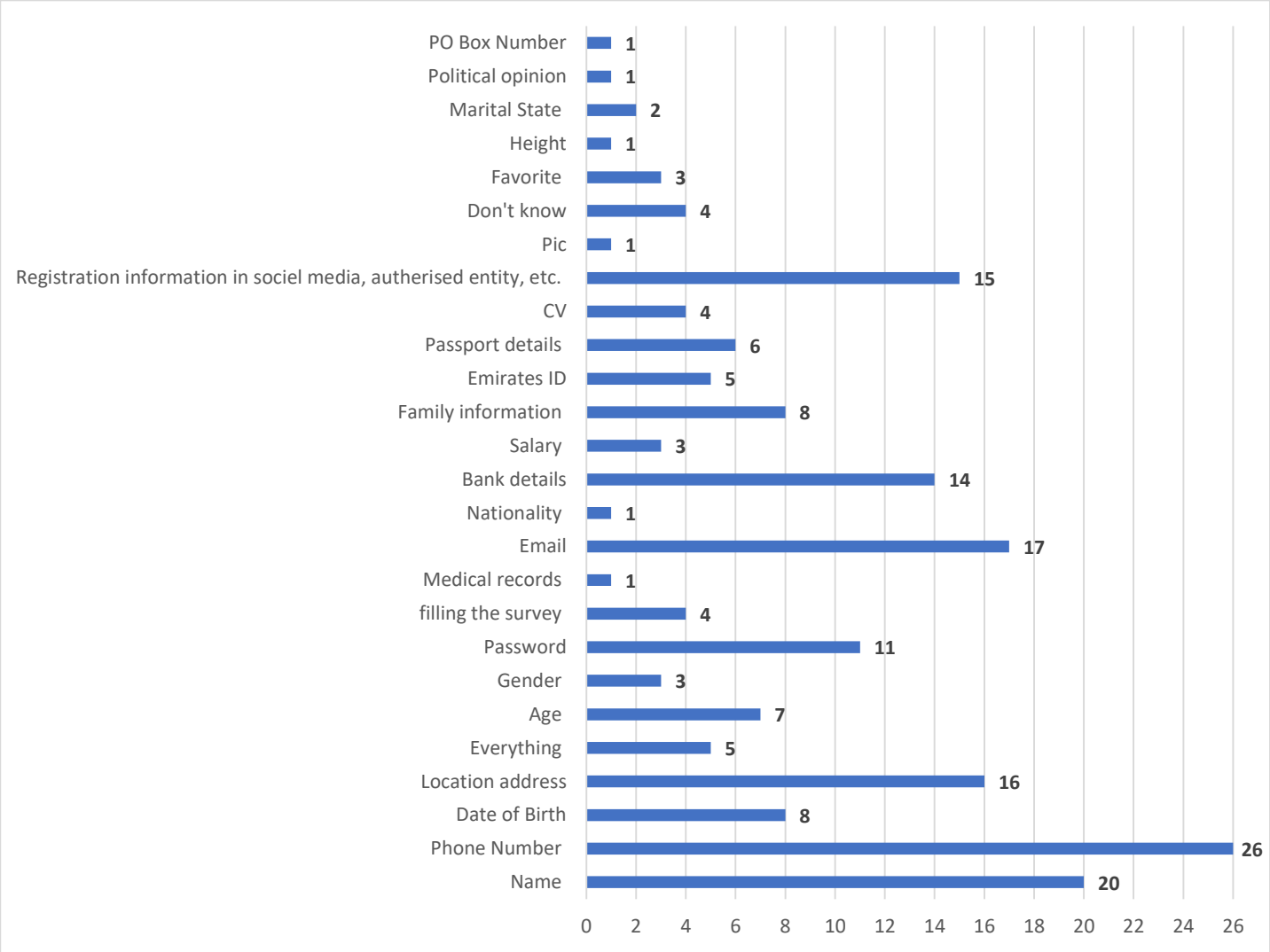


Figure 22: Data Types Shared by Respondents and Frequencies of the Sharing Personal Data
(Created by the Author)

Almost 44% of the respondents are willing to share their data with trusted companies and entities that follow a confidante privacy policy. However, 31.6% are not keen to share their data even if the company has a reliable privacy policy and 24.4% did not know if they were willing to share their data as presented in Figure 23. From the respondents' perspective, the

decision about sharing depends on the nature of the activity for which the data is needed. For example, if the sharing is for statistical purposes, the individual would be willing to share. However, if it is to be for influencing the market conditions, election polls, and/or such other social activity, the respondents expressed their preference not to share their data.

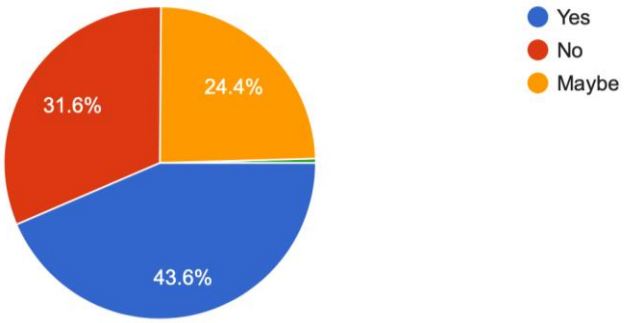


Figure 23: Percentage of People Willing to Share Their Personal Data with a Trusted Company
(Created by the Author)

Furthermore, figure 24 highlights the main factors that people verify before sharing their personal data. The main factors are the trust and confidence placed in the companies and persons and the people's knowledge about the applied data security and privacy policy through the companies' history and reputation. Also, it is important for the data provider to know about the purpose of using his/her data and to make sure that it is not shared with any third party for the company benefits. On the other hand, some of them indicated that if it is personal data then it should be shared with anyone.

In fact, there were almost similar percentages, 32.4% and 32.9% respectively, of the respondents who are ready to share their data to get a new service and personalised services, 33.3% preferred not to share their data to get a new service, and 30.7% did not want to share their data to get a new personalised service; 34.2% indicated that they might share their data to get a new service and 36.4% who might share their data to get a new personalised service. The data is presented in figures 25 and 26.

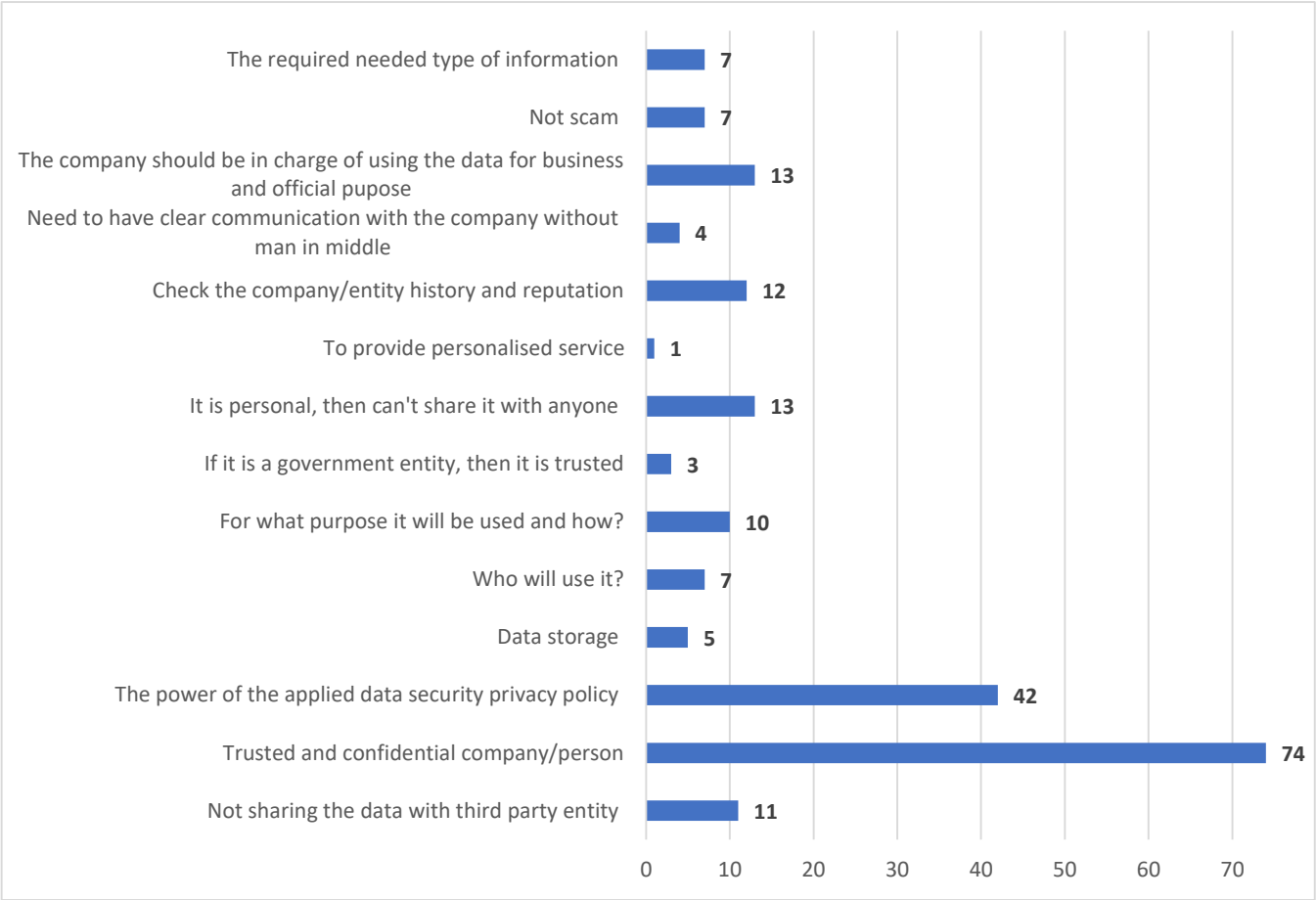


Figure 24: The Range of Main Factors That Led to Sharing Personal Data
(Created by the Author)

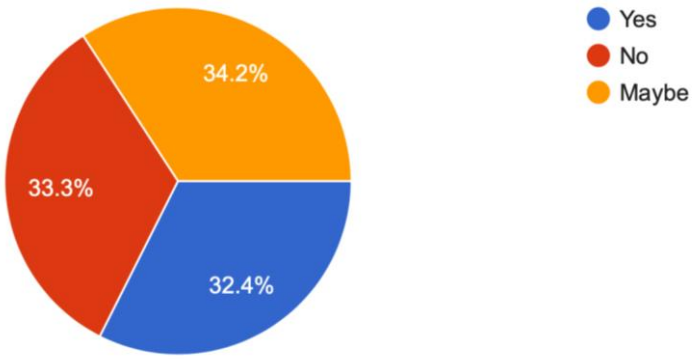


Figure 25: Percentage of People Willing to Share Their Personal Data to Get a New Service
(Created by the Author)

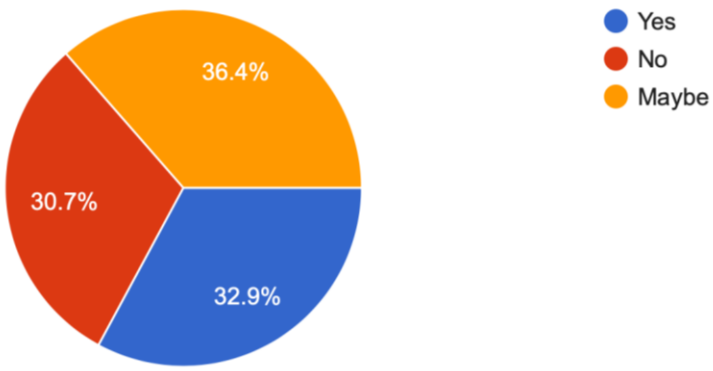


Figure 26: Percentage of People Willing to Share Their Personal Data to Get a New Personalised Service
(Created by the Author)

Also, people are keen to provide their personal data for the purpose of getting an offer in their interested services such as discount or coupon on their purchases or to receive special personalised services and offers. In this regard, Figure 28 shows that 24.9% were willing to share the data for this purpose, 40.9% were unwilling, while 33.8% might provide their data to get a unique offer as illustrated in figure 27.

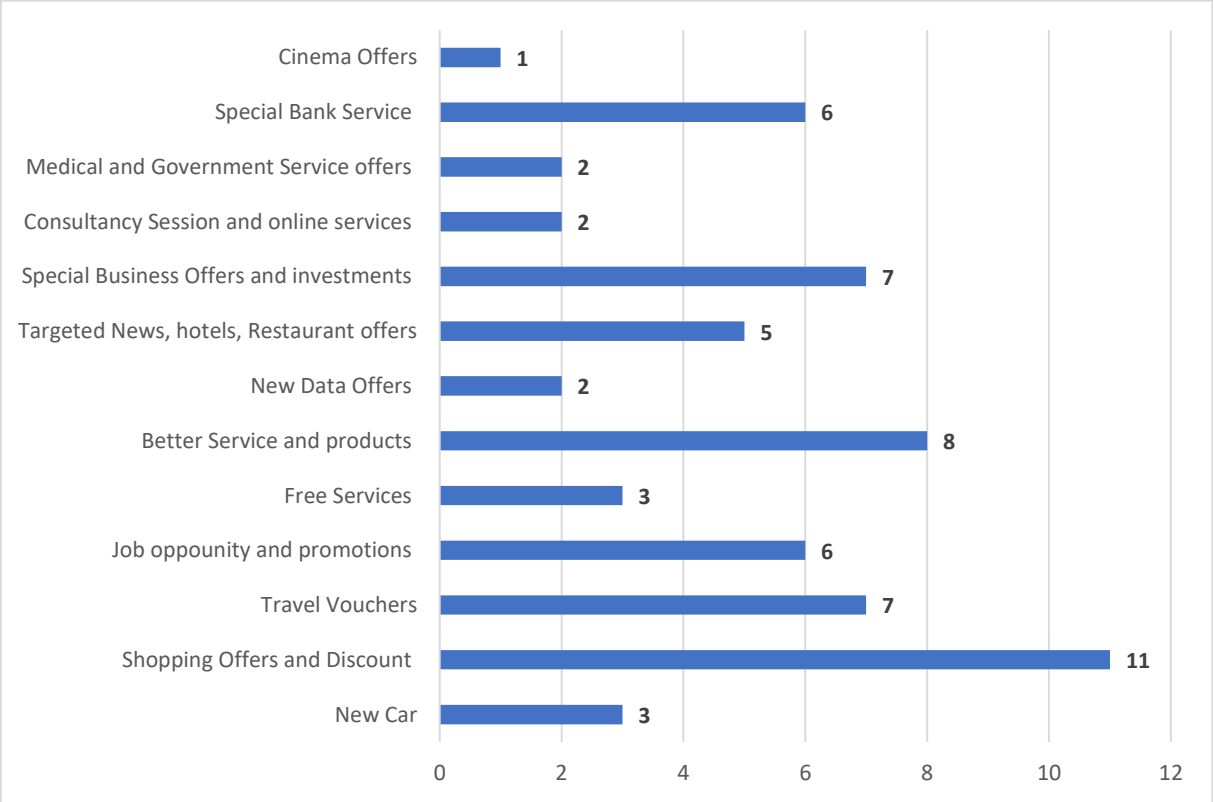


Figure 27: Respondents' Interest in Services for Which They are Willing to Provide Their Personal Data to Get an Offer in
(Created by the Author)

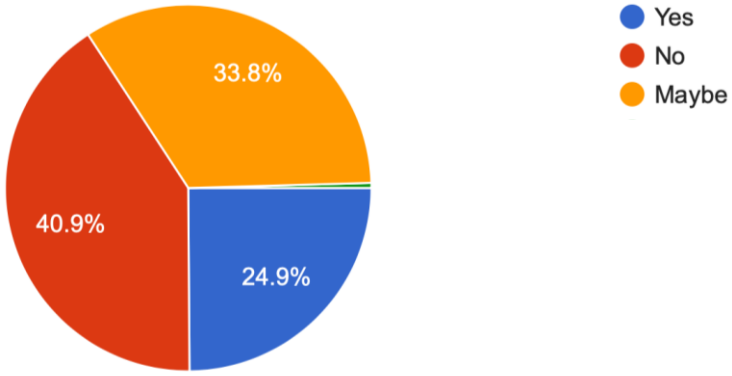


Figure 28: Percentage of People Willing to Share Their Personal Data to Get a New Offer on the Service of their Interest
(Created by the Author)

An investigation into the respondents' opinion on allowing a company to share their data with another company or a third party to provide them the best-enhanced services or offers showed that only 18.2% agreed to share the data with authenticated companies; however, a large number (60.9%) disagreed while 19.6% said they might agree if the company were to meet their demand and inform them before sharing their data. See figure 29.

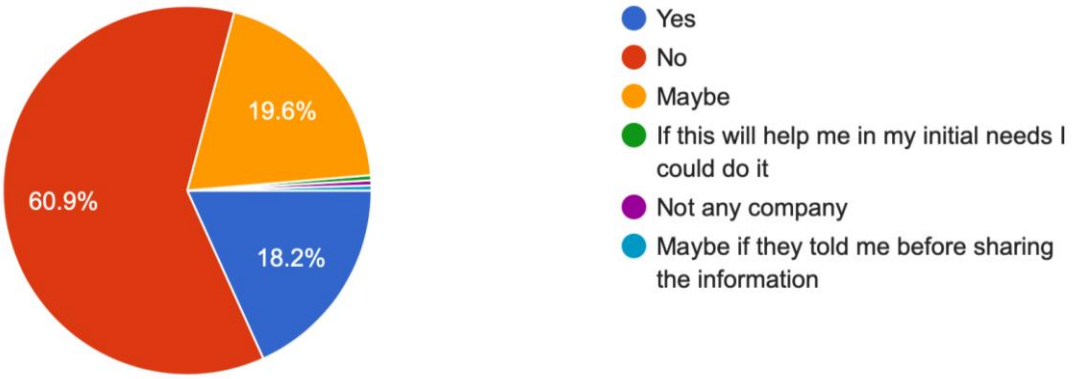


Figure 29: Percentage of People Willing to Share Their Personal Data with Other Companies to Get the Best-Enhanced Service or Offer
(Created by the Author)

Those who dismissed the idea of offering their data without getting paid or getting a special offer for it numbered 74.7%. However, 11.6% were willing to share their data with an authorised company without any benefits. Also, 13.3% were not sure about their decision. See figure 30.

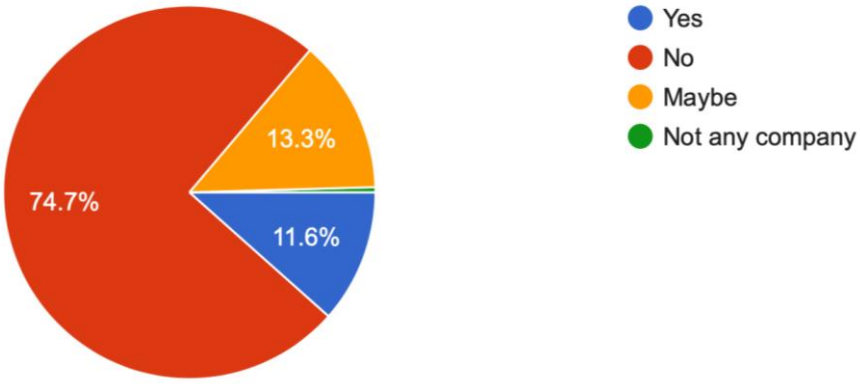


Figure 30: Percentage of People Willing to Share Their Personal Data with Other Companies Without Getting Paid, Special Service or Offers
(Created by the Author)

Although 54.7% of the respondents were not willing to share their personal data even if they were paid for it, 20.9% were ready to provide their data if they got paid for the requested data, and 24% were unsure about their decision as illustrated in figure 31.

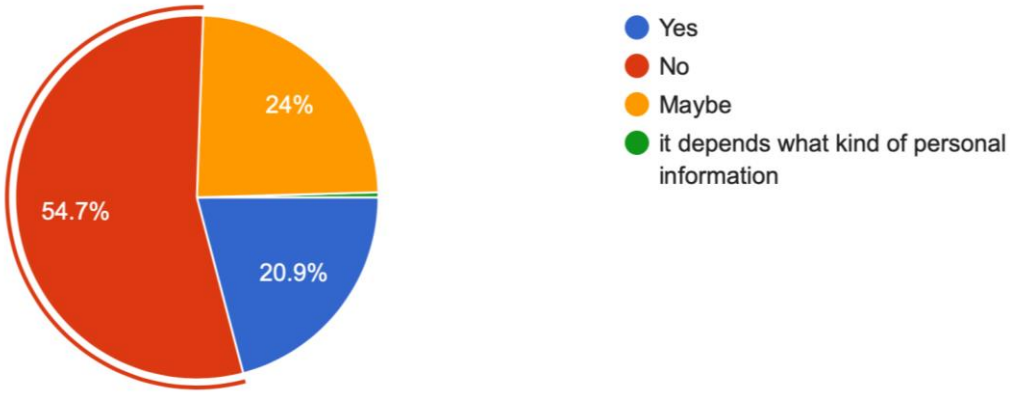


Figure 31: Percentage of People Who Agreed to Share Their Personal Data if They Get Paid
(Created by the Author)

Most of the respondents (72%) totally disagreed to get paid and gain money by offering their data and preferred to work or look for a job to earn money. However, 14.7% agreed, depending on the type of shared data. Also, 12.4% might share their data and get paid rather than work, as presented in figure 32.

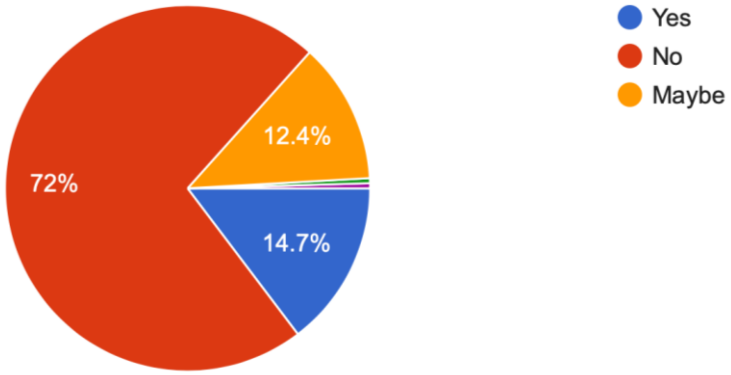


Figure 32: Percentage of People Who Agreed to Share Their Personal Data and Get Paid Rather Than Work
(Created by the Author)

Although 52.9% are willing to share their data only if they have the control to choose the personal data type and amount with a trustworthy person or company, almost half of the respondents disagree (23.6%) or might share even if they have the control (23.6%). See figure 33.

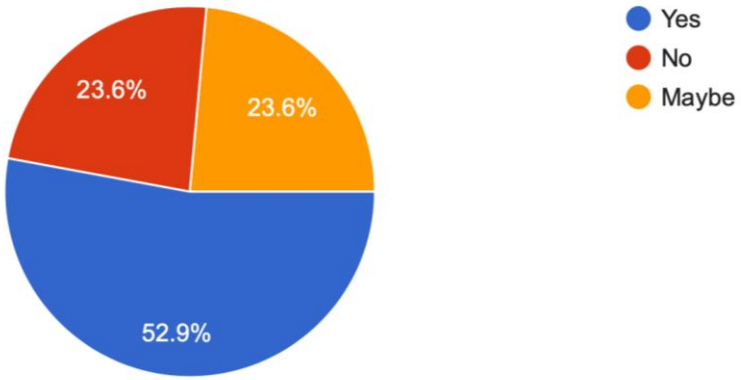


Figure 33: Percentage of People Who Agreed to Share Their Personal Data if They Have Control Over Their Shared Data
(Created by the Author)

Furthermore, nearly 37% of the respondents indicated their agreement to share their data for its protection with an insurance company while 34.2% disagreed and 28.4% were neutral in their opinion as illustrated in figure 34.

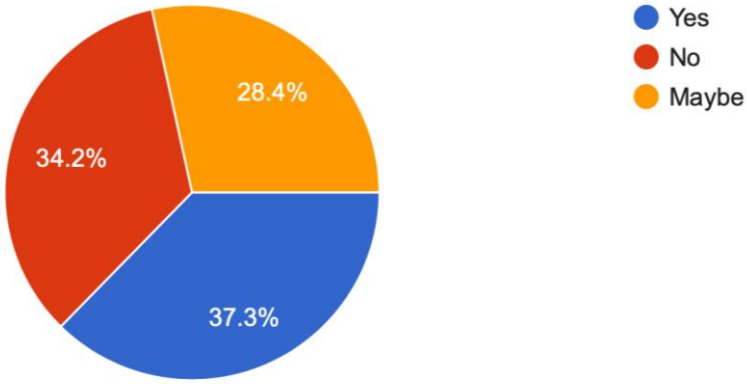


Figure 34: Percentage of People Who Agreed to Share Their Personal Data with an Insurance Company to Protect Their Data
(Created by the Author)

Besides, the survey investigated the main concerns and worries of sharing personal data. As shown in figure 35, the respondents' main concerns were over sharing their data with untrustworthy parties, hackers, and data thieves who use such data for their benefits or against the data provider by selling it, using it to commit fraud, and for other illegal purposes. Also, data leakage is critical as shared personal data is sometimes meant to be available to everyone without the data provider's permission and awareness. In addition, data providers should know about what will be done with their data, where it will be used, and for what purposes. Also, data providers are bothered and annoyed when they receive junk online advertisements and calls and if their data has been used without their receiving any benefits or personalised services. Finally, 6% of the responses indicated that if the data is called personal data, then that means it is personal and no one has the right to access or share it.

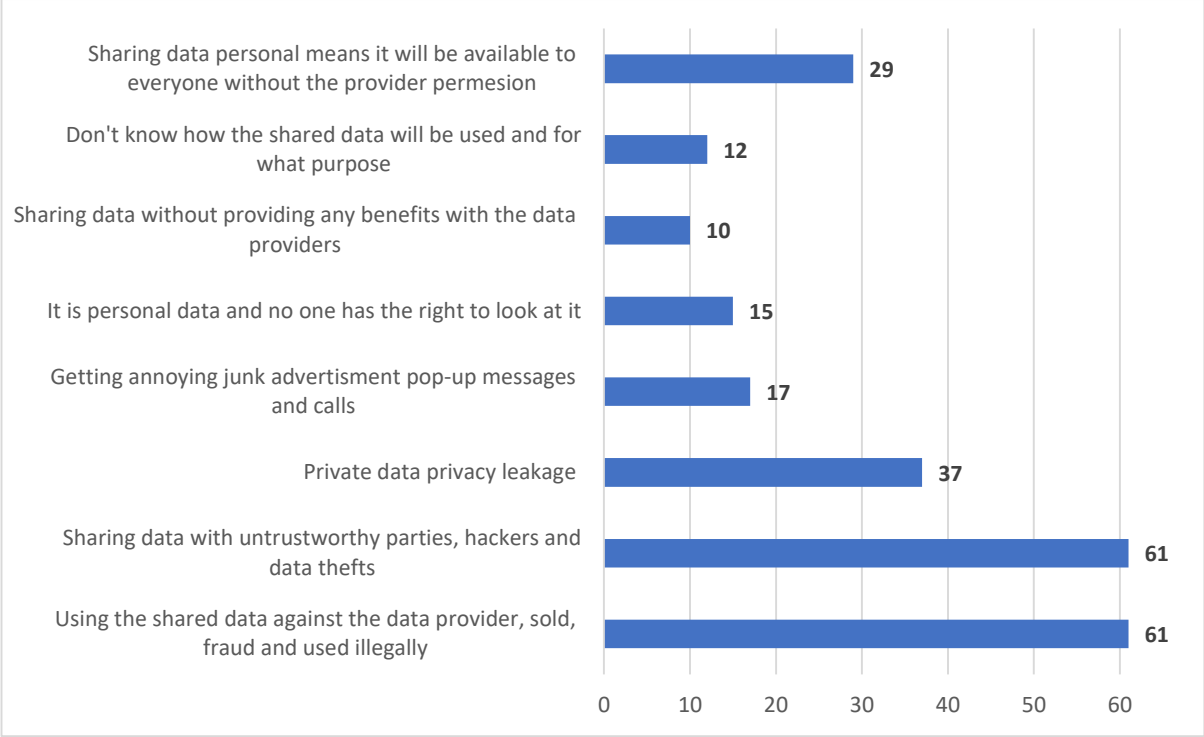


Figure 35: Respondents' Main Concerns and Worries of Sharing Their Personal Data
(Created by the Author)

5.1.3 Case Study Discussion

In the conducted survey, 225 respondents shared their point of view regarding sharing and monetising their personal data with different companies or people. Almost 50% of them were females between 18–24 years of age and held bachelor's degrees. They are from the UAE, employed and living in the UAE.

In addition, most of the respondents indicated they didn't share their personal data with anyone. However, some of them indicated that they shared their data such as their Names, Phone Numbers, Address, etc. Also, it was highlighted that people were willing to share their data with trusted entities such as government entities that apply and follow a reliable privacy policy guideline. Also, it is fine to share data if it is for demographic statistical records only and not for marketing or business.

Moreover, it was noticed that people have some concerns over sharing their data. It is essential to guarantee that the company/person is trusted and reliable as people should be aware of the security and privacy policy followed based on the history and reputation of the company. Also, it is critical for the data providers to know about what types of their data is classified as private data, and what may or may not be shared, and the uses to which their shared data would be put.

The survey results showed that the respondents' opinions are similar regarding sharing their data for the purpose of receiving a new general or new personalised service. Nevertheless, most of them disagreed over sharing their data in order to get a new offer on the services or the best and enhanced services and offers from third-party companies.

Besides, they were unwilling to share their data even if they get paid; in case if they had to share their data, then totally disagreed with providing their data without getting paid or receiving a special offer. Also, they prefer to get money from their work rather than from their data monetisation.

In fact, the respondents are keen to participate with their data only if they have the control and ownership over selecting the exact personal data to be shared with a trustworthy person or company. Also, they seek an insurance company to protect their data and maintain their data-sharing concerns.

5.1.3.1 Data Protection Law in the UAE

Ford (2018) stated that there are no federal data protection laws in the UAE nor a national data protection regulator; however, there are a several national and sectoral laws related to data protection and privacy.

5.1.3.1.1 **National laws**

National data protection and privacy laws include the following as per Ford (2018):

- "Article 31 of the UAE's constitution guarantees the secrecy and freedom of communication by post, telegraph or "other means of communication".
- "Article 378 of the 1987 Penal Code states that the publication of personal data relating to individuals' private or family life is an offence punishable by detention and a fine".

In addition, the cybercrimes law (Federal Decree-Law no. (5) of 2012 on Combating Cybercrimes) sets a number of penalties of specific activities related to hacking and data protection[4].

5.1.3.1.2 **Sectoral laws**

The Telecommunications Regulatory Authority (TRA) has regulated electronic transactions and commerce. The TRA initiated several laws related to consumer data protection, regulatory and electronic transactions, and commerce law[5].

5.1.3.1.3 **The DHC and DIFC**

There are two free zones in Dubai, Dubai Healthcare City (DHC) and Dubai International Financial Centre (DIFC), which follow their own data protection laws as follows:

"The DHC is regulated by the Health Data Protection Regulation (Regulation No. 7 of 2013), and data protection in the DIFC is regulated by DIFC Data Protection Law – Law No.

[4] Federal Decree-Law no. (5) of 2012 accessed on 15 Jun 2019 at http://ejustice.gov.ae/downloads/latest_laws/cybercrimes_5_2012_en.pdf
[5] TRA laws accessed on 15 Jun 2019 at https://www.tra.gov.ae/en/about-tra/legal-references/law.aspx

1 of 2007 as amended by DIFC Law No. 5 of 2012 and the DPR (Data Protection Regulations – Consolidated Version No.2 In force on 23.12.2012).” (Ford 2018)

5.1.3.1.4 **GDPR**

All organisations in the UAE and Gulf which processed EU residents’ personal data should follow EU GDPR[6].

5.1.3.1.5 **Smart Dubai**

It is the main element in the vision of His Highness Sheikh Mohammed Bin Rashid Al Maktoum, Vice-President and Prime Minister of the UAE, and Ruler of Dubai, to make Dubai the happiest city worldwide.

Hence, the Dubai Data initiative is the key to enabling the happiness vision. It is the most exhaustive and resourceful data initiative worldwide. Its aim is to collect data from the different government and private entities in Dubai, in order to drive well-informed knowledge to empower all stakeholders, enhance the quality of life, and lead the new economic wave.

Dubai Data offers the Dubai Pulse platform, which provides open data in Dubai. Such a platform affords accessibility to the city data across different entities, with 405 datasets along with data city and people flow. However, according to the expert in the Smart Dubai Office, all the provided data are anonymous as per the data law and by merging and processing different datasets, they have made sure that, even if anyone tries to find the exact owner of the data, the person will not succeed.

[6] EU GDPR Guide accessed on 15 Jun 2019 at https://www.itgovernancegulf.com/shop/Product/eu-gdpr-a-pocket-guide

6 Chapter Six: Conclusion and Future work

This chapter presents an overall conclusion of the personal data monetisation concept and its existing aspects and challenges. Also, it highlights the work done on the subject, the recommendations arising from the work, limitations and future work possibilities.

6.1 Conclusion

This dissertation focuses on the personal data monetisation procedure which will act as the future economic accelerator worldwide. Each generated data has an economic value, which affects the different related entities.

Hence, the first aim of this study is to explore the essential components in order to build an effective data monetisation strategy in the city of Dubai and the UAE. This has been addressed in chapter 2 in the literature review in which significant academic studies and technical technological trend reports have been explored. The results of the literature survey are reported and the data strategy structure is initiated, which includes data types, city's policy, changing the city's partners, strategic pathway, strategy themes, and framing data monetisation strategy along with its challenges, success factors, integration, and managers' skills. Also, data monetisation business models including data monetisation procedures, impact, outcome, generating new revenue, and emerging new products or services are explored.

Moreover, the second aim is to discover the current personal data monetisation strategies, procedures, and platforms that have been applied and have achieved the targeted outcomes. This aim has been achieved by following the systematic review methodology that includes several steps and processes as mentioned in Chapter 3. The beginning was made by searching for the relevant studies from the four significant databases based on the selected keywords, then filtering the studies collection as per the inclusion and exclusion criteria, applying the quality assessment, data coding, and analysis. The filtered 182 major published

researches, which had been published during the past 17 years were assessed, processed, and analysed. The results of the analysis are presented in Chapter 4. The conducted quantitative research results in the answers to this study's research questions, which related to the personal data monetisation process as follows:

1. The co-related definitions include
    a. Personal Data
    b. Personally Identifiable Information (PII)
    c. Personal Information
    d. Personal Information Management
    e. Personal Service Data
    f. Personal Informatics (PI) Technologies
    g. Personal Data Store (PDS)
    h. Personal Data Lake
    i. Data Brokers
    j. Data Monetisation Concept
2. The common aims are to overcome security concerns, make recommendations, and observe the user's behaviour to reshape the industry and marketplace and enhance the quality of life.
3. The common problems are: most of the data providers lose control on their data and there is lack of privacy and provider's knowledge of their monetisation and usage as well as the data storage, trading, and exposure in the IoT network concerns.
4. The common challenge is the personal data collection and storing process along with data security as well as the awareness of the economic power of the generated personal data.
5. The main affecting factors are related to the user's willingness to share their data, including the trust relationship, and maintaining their privacy. Also, the related factors of the user's

behaviour tracking and recommendation services including technical, legal, social, and psychological factors.

6. The major existing related work includes the two-sided trading market platforms and maintains personal data anonymisation as well as the protection procedures which consist of several protection bodies across different countries and the data protection process by the untrusted entity. Also highlighted is the personal data value, which acts as the new currency.
7. The common methodology used by the scholars to process the personal data is mainly through conducting surveys. The focus on the personal data monetisation has increased in 2019.
8. The common outcomes are to provide the best-personalised services and offers by tracking the user's activities and driving innovation and economic growth.
9. The most supported countries are mainly the EU member countries, US, and China.
10. The main context that applied the personal data monetisation are the online mobile-based interactions, healthcare, data security, privacy protection, economic challenges, travel and tourism, IoT services, and leisure activities.
11. The customer's main concerns are essentially anything that is related to their data privacy protection techniques as well as the power of the trusted and confident relationship with the data consumers.

Furthermore, the third aim is to investigate the citizens' awareness of their personal data monetisation process and their knowledge about the outcome value in addition to the people's acceptance to distribute their personal data. This objective is related to research question No. 4 of this study and answered in Chapter 5. A case study of the UAE has been conducted by publishing an online survey answered by UAE citizens. The case study covers the demographic data and research questionnaire. The overall result indicates that the UAE

citizens are unwilling to provide their personal data unless they have control and ownership to reveal the exact data that they want to share and receive benefits based on the shared data.

6.2 Recommendations

It is recommended from each city, organisation, and entity which has a vision of driving the smartest services and maintain their users and residents' happiness, to apply personal data monetisation procedure and data strategy structure. This can be achieved by selecting the relevant data types, setting the effective city's data policy, electing the efficient partners, picking the right significant strategic pathway, and following the strategic structure themes in order to frame the powerful data monetisation strategy.

Furthermore, it is essential for each personal data monetisation procedure to overcome the existing challenges and data providers' concerns to be able to engage in the data economic growth and enhance the quality of life. This could be achieved through providing a controlled unified platform jointly for data providers and data consumers to be able to trade their data in a trusted, confidential, and secured approach as well as to guarantee that each data provider will be rewarded in the form of valuable cash, business benefits, personalised services, and superior suggestions based on the provided amount of data. The user's privacy, data sensitivity, and information anonymisation will also be taken into consideration.

6.3 Limitations and Future Work

The study's limitations are that some of the research doesn't differentiate between general data monetisation and personal data monetisation, thus a hard check and paper review is required to retrieve the required relevant information related to the study objectives. Also, further research and exploration is required through the other databases to get more information. In addition, the future work will be focused on a specific organisation which

applies the personal data monetisation in order to explore the procedure activities and practices in the UAE and investigates the opinion of the data consumers during the monetisation process.

References

Adjei, J. K. (2014). Explaining the role of trust in cloud service acquisition. *In 2014 2nd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering*. Oxford, UK: IEEE, pp. 283–288.

Adjei, J. K. (2016). Monetization of personal identity information: Technological and regulatory framework. *In 2015 2nd International Conference on Information Science and Security (ICISS)*. Seoul, South Korea: IEEE.

Adler, R., Stringer, C. & Yap, M. (2016). The valuation and pricing of information assets. *Pacific Accounting Review*, vol. 28(4), pp. 419–430.

Al-emran, M., Mezhuyev, V. & Kamaludin, A. (2018). Technology acceptance model in m-learning context : a systematic review. *Computers & Education*, vol. 125(August), pp. 389–412.

Al-emran, M., Mezhuyev, V., Kamaludin, A. & Shaalan, K. (2018). The impact of knowledge management processes on information systems : a systematic review. *International Journal of Information Management*, vol. 43(August), pp. 173–187.

Aldhouse, F. (2014). Anonymisation of personal data - a missed opportunity for the European Commission. *Computer Law and Security Review*, vol. 30(4), pp. 403–418.

Alkhatib, M., Barachi, M. El & Shaalan, K. (2018). Using arabic social media feeds for incident and emergency management in smart cities. *In 2018 3rd International Conference on Smart and Sustainable Technologies (SpliTech)*. Split, Croatia: IEEE, pp. 1–6.

Alsahafi, A. Y. A. & Gay, B. V. (2018). An overview of electronic personal health records. *Health Policy and Technology*, vol. 7(4), pp. 427–432.

Anciaux, N., Bonnet, P., Bouganim, L. & Nguyen, B. (2019). Personal data management systems : the security and functionality standpoint. *Information Systems*, vol. 80, pp. 13–35.

Anciaux, N., Nguyen, B. & Popa, I. S. (2013). Personal data management with secure hardware: how to keep your data at hand. *In 2013 IEEE 14th International Conference on Mobile Data Management*. Milan, Italy: IEEE, pp. 1–2.

Bae, S. H. & Kim, J. (2010). Personal information protection model based on mobile agent. *In 2010 Seventh International Conference on Information Technology: New Generations*. Las Vegas, NV, USA: IEEE, pp. 719–724.

Baird, C. H. & Parasnis, G. (2011). From social media to social customer relationship management. *Strategy and Leadership*, vol. 39(5), pp. 30–37.

Baloyi, N. & Kotze, P. (2017a). Are organisations in South Africa ready to comply with personal data protection or privacy legislation and regulations? *In 2017 IST-Africa Week Conference (IST-Africa)*. Windhoek, Namibia: IEEE, pp. 1–11.

Baloyi, N. & Kotze, P. (2017b). Do users know or care about what is done with their personal data: a South African study. *In 2017 IST-Africa Week Conference (IST-Africa)*. Windhoek, Namibia: IEEE, pp. 1–11.

Barsky, J. (2018). Fishing for whales: a segmentation model for social casinos. *International Journal of Quality and Service Sciences*, vol. 10(4), pp. 400–421.

Bataineh, A. S., Mizouni, R., El Barachi, M. & Bentahar, J. (2016). Monetizing personal data: a two-sided market approach. *Procedia Computer Science*, vol. 83(Ant), pp. 472–479.

Becker, M. J. (2014). The consumer data revolution : the reshaping of industry competition and a new perspective on privacy. *Journal of Direct, Data and Digital Marketing Practice*,

vol. 15(3), pp. 213–218.

Beldad, A., De Jong, M. & Steehouder, M. (2011). I trust not therefore it must be risky: determinants of the perceived risks of disclosing personal data for e-government transactions. *Computers in Human Behavior*, vol. 27(6), pp. 2233–2242.

Berman, S. J., Battino, B. & Feldman, K. (2011). New business models for emerging media and entertainment revenue opportunities. *Strategy and Leadership*, vol. 39(3), pp. 44–53.

Biliri, E., Kokkinakos, P., Michailitsi, A., Papaspyros, D., Tsapelas, J., Mouzakitis, S., Koussouris, S., Lampathaki, F., Glickman, Y. & Kirstein, F. (2018). Big data analytics in public safety and personal security: challenges and potential. *In 2017 International Conference on Engineering, Technology and Innovation (ICE/ITMC)*. Funchal, Portugal: IEEE, pp. 1382–1386.

Bolton, R. N., McColl-Kennedy, J. R., Cheung, L., Gallan, A., Orsingher, C., Witell, L. & Zaki, M. (2018). Customer experience challenges: bringing together digital, physical and social realms. *Journal of Service Management*, vol. 29(5), pp. 776–808.

Bradford, M., Earp, J. B. & Williams, P. F. (2017). Understanding sustainability for socially responsible investing and reporting. *Journal of Capital Markets Studies*, vol. 1(1), pp. 10–35.

Brier, J. (2017). Defining the limits of governmental access to personal data stored in the cloud: an analysis and critique of Microsoft Ireland. *Journal of Information Policy*, vol. 7(2017), p. 327.

Carrascal, J. P., Riederer, C., Erramilli, V., Cherubini, M. & de Oliveira, R. (2013). Your browsing behavior for a big mac: economics of personal information online. *In Proceedings of the 22nd international conference on World Wide Web*. Rio de Janeiro, Brazil, pp. 189–200.

Cha, S. C. & Yeh, K. H. (2018). A data-driven security risk assessment scheme for personal data protection. *IEEE Access*. IEEE, vol. 6, pp. 50510–50517.

Chen, Y.-C. & Kao, S.-J. (2006). Application services based on personal data ontology. *In 5th IEEE/ACIS International Conference on Computer and Information Science and 1st IEEE/ACIS International Workshop on Component-Based Software Engineering,Software Architecture and Reuse (ICIS-COMSAR'06)*. Honolulu, HI,: IEEE, pp. 280–285.

Chessa, M. & Loiseau, P. (2017). A cooperative game-theoretic approach to quantify the value of personal data in networks. *In Proceedings of the 12th workshop on the Economics of Networks, Systems and Computation*. Cambridge, Massachusetts: ACM, p. 9.

Chipp, K. F. & Chakravorty, D. (2016). Producer push to consumer pull: who curates new media content? developing strategies for new media environments. *Journal of Product and Brand Management*, vol. 25(4), pp. 373–386.

Choi, H. S., Lee, W. S. & Sohn, S. Y. (2017). Analyzing research trends in personal information privacy using topic modeling. *Computers and Security*, vol. 67, pp. 244–253.

Choi, J. P., Jeon, D. S. & Kim, B. C. (2019). Privacy and personal data collection with information externalities. *Journal of Public Economics*, vol. 173, pp. 113–124.

Chowdhury, M. J. M., Colman, A., Kabir, M. A., Han, J. & Sarda, P. (2018). Blockchain as a notarization service for data sharing with personal data store. *In 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*. New York, NY, USA: IEEE, pp. 1330–1335.

Chua, H. N., Wong, S. F., Chang, Y. & Libaque-Saenz, C. F. (2017). Unveiling the coverage

patterns of newspapers on the personal data protection act. *Government Information Quarterly*, vol. 34(2), pp. 296–306.

Cooper, T. & LaSalle, R. (2016). Guarding and growing personal data value, pp. 1–32 [online].Available at: https://www.accenture.com/_acnmedia/PDF-4/Accenture-Guarding-and-Growing-Personal-Data-Value-POV-Low-Res.pdf#zoom=50.

Cummins, S., Peltier, J. W., Schibrowsky, J. A., Nill, A., Cummins, S. & Peltier, J. W. (2014). Consumer behavior in the online context. *Journal of Research in Interactive Marketing*, vol. 8(3), pp. 169–202.

Dann, D., Teubner, T. & Weinhardt, C. (2019). Poster child and guinea pig – insights from a structured literature review on Airbnb. *International Journal of Contemporary Hospitality Management*, vol. 31(1), pp. 427–473.

Dimakopoulos, P. & Sudaric, S. (2017). *User data and platform competition*. International Journal of Industrial Organization.

Dinero, J. & Chua, H. N. (2018). Predicting personal mobility data disclosure. *In 2018 IEEE Conference on Big Data and Analytics (ICBDA)*. Langkawi Island, Malaysia: IEEE, pp. 50–55.

Dong, X., Guo, B., Duan, X., Shen, Y., Zhang, H. & Shen, Y. (2017). DSPM: a platform for personal data share and privacy protect based on metadata. *In 2016 13th International Conference on Embedded Software and Systems (ICESS)*. Chengdu, China: IEEE, pp. 182–185.

Elliot, M., O'Hara, K., Raab, C., O'Keefe, C. M., Mackey, E., Dibben, C., Gowans, H., Purdam, K. & McCullagh, K. (2018). Functional anonymisation: personal data and the data environment. *Computer Law and Security Review*, vol. 34(2), pp. 204–221.

Elmisery, A. M., Rho, S. & Botvich, D. (2015). A distributed collaborative platform for personal health profiles in patient-driven health social network. *International Journal of Distributed Sensor Networks*, vol. 11(9), p. 406940.

Estrada-Jiménez, J., Parra-Arnau, J., Rodríguez-Hoyos, A. & Forné, J. (2019). On the regulation of personal data distribution in online advertising platforms. *Engineering Applications of Artificial Intelligence*, vol. 82(March), pp. 13–29.

Evens, T. & Damme, K. Van. (2016). Consumers ' willingness to share personal data : implications for newspapers ' business models. *International Journal on Media Management*. Routledge, vol. 18(1), pp. 25–41.

Faber, B., Michelet, G. C., Weidmann, N., Mukkamala, R. R. & Vatrapu, R. (2019). BPDIMS: a blockchain-based personal data and identity management system. *Proceedings of the 52nd Hawaii International Conference on System Sciences*. Wailea, United States: Hawaii International Conference on System Sciences (HICSS), pp. 6855–6864.

Fahy, R., Van Hoboken, J. & Van Eijk, N. (2018). Data privacy, transparency and the data-driven transformation of games to services. *In 2018 IEEE Games, Entertainment, Media Conference (GEM)*. Galway, Ireland: IEEE, pp. 136–146.

Feijóo, C., Gómez-Barroso, J. L. & Voigt, P. (2014). Exploring the economic value of personal information from firms' financial statements. *International Journal of Information Management*, vol. 34(2), pp. 248–256.

Feri, F., Giannetti, C. & Jentzsch, N. (2016). Disclosure of personal information under risk of privacy shocks. *Journal of Economic Behavior and Organization*, vol. 123, pp. 138–148.

Ford, N. (2018). *Data protection law in the UAE*. *IT Governance Gulf* [online]. [Accessed 15

June 2019]. Available at: https://www.itgovernancegulf.com/blog/data-protection-law-in-the-uae.

Fortin, D. & Uncles, M. (2011). The first decade : emerging issues of the twenty-first century in consumer marketing. *Journal of Consumer Marketing*, vol. 28(7), pp. 472–475.

Forum, W. E. & Kearney, A. T. (2014). *Rethinking personal data: a new lens for strengthening trust*. Cologny, Switzerland: World Economic Forum [online].Available at: http://reports.weforum.org/rethinking-personal-data/.

Foster, J. (2016). Towards an understanding of data work in context: emerging issues of economy, governance, and ethics. *Library Hi Tech*, vol. 34(2), pp. 182–196.

Francis, L. P. & Francis, J. G. (2017). Data reuse and the problem of group identity. *Studies in Law Politics and Society*, vol. 73, pp. 141–164.

Frecè, J. T. & Selzam, T. (2017). Tokenized ecosystem of personal data — exemplified on the context of the smart city. *JeDEM-eJournal of eDemocracy and Open Government*, vol. 9(2), pp. 110–133.

Fred, J. (2017). *Data monetization - how an organization can generate revenue with data?* Tampere University of Technology, Master's theses [online].Available at: https://dspace.cc.tut.fi/dpub/bitstream/handle/123456789/24694/fred.pdf?sequence=1&isAllowed=y.

Frey, R. M., Buhler, P., Gerdes, A., Hardjono, T., Fuchs, K. L. & Ilic, A. (2017). The effect of a blockchain-supported, privacy-preserving system on disclosure of personal data. *In 2017 IEEE 16th International Symposium on Network Computing and Applications (NCA)*. Cambridge, MA, USA: IEEE, pp. 1–5.

Gabisch, J. A. & Milne, G. R. (2014). The impact of compensation on information ownership and privacy control. *Journal of Consumer Marketing*, vol. 31(1), pp. 13–26.

Galbreath, J. (2002). Success in the relationship age : building quality relationship assets for market value creation. *The TQM Magazine*, vol. 14(1), pp. 8–24.

Gandhi, A., Sucahyo, Y. G. & Ruldeviyani, Y. (2019). Investigating the protection of customers' personal data in the ridesharing applications: a desk research in Indonesia. *In 2018 15th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON)*. Chiang Rai, Thailand: IEEE, pp. 118–121.

García, A., Dominguez, F., Calle, L., Martinez, J. & Raymundo, C. (2018). Personal data protection maturity model for the micro financial sector in Peru. *International Journal of Engineering Research and Technology*, vol. 11(4), pp. 649–660.

Geissbuhler, A., Safran, C., Buchan, I., Bellazzi, R., Labkoff, S., Eilenberg, K., Leese, A., Richardson, C., Mantas, J., Murray, P. & De Moor, G. (2013). Trustworthy reuse of health data: a transnational perspective. *International Journal of Medical Informatics*, vol. 82(1), pp. 1–9.

Gerlach, J., Widjaja, T. & Buxmann, P. (2015). Handle with care: how online social network providers' privacy policies impact users' information sharing behavior. *Journal of Strategic Information Systems*, vol. 24(1), pp. 33–43.

Ghosh, I. & Singh, V. (2018). Phones, privacy, and predictions: a study of phone logged data to predict privacy attitudes of individuals. *Online Information Review* [online].Available at: https://doi.org/10.1108/ OIR-03-2018-0112.

González-Manzano, L., González-Tablas, A. I., De Fuentes, J. M. & Ribagorda, A. (2014).

CooPeD: co-owned personal data management. *Computers and Security*, vol. 47(December 2013), pp. 41–65.

Granic, A. & Marangunic, N. (2015). Technology acceptance model : a literature review from 1986 to 2013. *Universal Access in the Information Society*, vol. 14(1), pp. 81–95.

Grodzinsky, F., Gumbus, A. & Lilley, S. (2013). Will "smarter" marketing end social discrimination? a critical review. *Journal of Information, Communication and Ethics in Society*, vol. 11(3), pp. 132–143.

Guo, A. & Ma, J. (2017). Context-aware scheduling in personal data collection from multiple wearable devices. *IEEE Access*, vol. 5, pp. 2602–2614.

Halej, J. (2017). *Ethics in primary research (focus groups, interviews and surveys). ECU Research and Data Briefing*. United Kingdom [online].Available at: https://warwick.ac.uk/fac/cross_fac/ias/activities/accolade/resources/ecu_research_ethics.pdf.

Han, S. (2015). Study on the legal protection of personal information and its free movement in electronic commerce. *In 2015 Fifth International Conference on Communication Systems and Network Technologies*. Gwalior, India: IEEE, pp. 1360–1364.

Haynes, D., Bawden, D. & Robinson, L. (2016). A regulatory model for personal data on social networking services in the UK. *International Journal of Information Management*, vol. 36(6), pp. 872–882.

Hernández-Ramos, J. L., Pérez, S., Hennebert, C., Bernabé, J. B., Denis, B., Macabies, A. & Skarmeta, A. F. (2018). Protecting personal data in IoT platform scenarios through encryption-based selective disclosure. *Computer Communications*, vol. 130(July), pp. 20–37.

Hertzfeld, E. (2017). Data leads to monetization, personalization. *Hotel Management (21582122)*. United States of America: Questex Media Group, p. 52.

Hildebrandt, M., O'Hara, K. & Waidner, M. (2013). *Digital enlightenment yearbook 2013: the value of personal data*. reprint. IOS Press.

Hirsch, P. B. (2019). The goose that laid the golden eggs: personal data and the Internet of Things. *Journal of Business Strategy*, vol. 40(1), pp. 48–52.

Van Hoboken, J. (2016). From collection to use in privacy regulation? a forward-looking comparison of european and us frameworks for personal data processing. *Exploring the Boundaries of Big Data*, pp. 231–259.

Hopia, H., Punna, M., Laitinen, T. & Latvala, E. (2015). A patient as a self-manager of their personal data on health and disease with new technology - challenges for nursing education. *Nurse Education Today*, vol. 35(12), pp. e1–e3.

Hornik, J., Shaanan Satchi, R. & Rachamim, M. (2019). The joy of pain: a gloating account of negative electronic word-of-mouth communication following an organizational setback. *Internet Research*, vol. 29(1), pp. 82–103.

Huddleston Jr, T. (2014). *Study: americans lament loss of privacy, but still share freely online. Fortune* [online]. [Accessed 25 May 2019]. Available at: http://fortune.com/2014/11/12/study-americans-lament-loss-of-privacy-but-still-share-freely-online/.

Hustinx, P. (2014). Privacy and competitiveness in the age of big data: the interplay between data protection, competition law and consumer protection in the digital economy. *European Data Protection Supervisor (EDPS)*. Brussels [online].Available at: www.edps.europa.eu.

Information Builders. (2018). *Data monetization strategies: how to make money or save*

money with data and analytics. *Information Builders*. New York [online].Available at: https://www.gartner.com/it-glossary/data-monetization.

Jammalamadaka, R. C., Mehrotra, S. & Venkatasubramanian, N. (2011). Protecting personal data from untrusted web-based data services. *Network Security*, vol. 2011(9), pp. 11–16.

Johnson, J. S., Friend, S. B. & Lee, H. S. (2017). Big data facilitation, utilization, and monetization: exploring the 3Vs in a new product development process. *Journal of Product Innovation Management*, vol. 34(5), pp. 640–658.

Kabanov, I. (2016). Effective frameworks for delivering compliance with personal data privacy regulatory requirements. *In 2016 14th Annual Conference on Privacy, Security and Trust (PST)*. Auckland, New Zealand: IEEE, pp. 551–554.

Kamaruddin, A., Dix, A. & Razak, F. H. A. (2011). Using diary to uncover users' personal information management (PIM) behaviours. *Proceedings - 2011 International Conference on User Science and Engineering, i-USEr 2011*. IEEE, pp. 201–205.

Karampela, M., Ouhbi, S. & Isomursu, M. (2018). Personal health data: a systematic mapping study. *International Journal of Medical Informatics*, vol. 118, pp. 86–98.

Kasavana, M. L., Nusair, K. & Teodosic, K. (2010). Online social networking: redefining the human web. *Journal of Hospitality and Tourism Technology*, vol. 1(1), pp. 68–82.

Kasuya, S., Zhou, X., Tago, K., Nishimura, S. & Jin, Q. (2017). Cyber-enabled well-being oriented daily living support based on personal data analytics. *IEEE Transactions on Emerging Topics in Computing*. IEEE, p. 1.

Katulic, T. & Katulic, A. (2018). GDPR and the reuse of personal data in scientific research. *In 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*. Opatija, Croatia: IEEE, pp. 1311–1316.

Kelley, T. & Bertenthal, B. I. (2016). Attention and past behavior, not security knowledge, modulate users' decisions to login to insecure websites. *Information and Computer Security*, vol. 24(2), pp. 164–176.

Kennedy, A. M. & Laczniak, G. R. (2016). Conceptualisations of the consumer in marketing thought. *European Journal of Marketing*, vol. 50(1–2), pp. 166–188.

Khovanskaya, V., Baumer, E. P. S., Cosley, D., Voida, S. & Gay, G. (2013). everybody knows what you're doing : a critical design approach to personal informatics. *CHI '13 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. Paris, France: ACM, pp. 3403–3412.

Kim, D., Park, K., Park, Y. & Ahn, J. H. (2019). Willingness to provide personal information: perspective of privacy calculus in IoT services. *Computers in Human Behavior*, vol. 92(August 2018), pp. 273–281.

Kim, K. K., Lee, A. R. & Lee, U. K. (2019). Impact of anonymity on roles of personal and group identities in online communities. *Information and Management*, vol. 56(1), pp. 109–121.

Kim, M. S. & Kim, S. (2018). Factors influencing willingness to provide personal information for personalized recommendations. *Computers in Human Behavior*, vol. 88(June), pp. 143–152.

Kim, T. K. & Choi, M. (2019). Older adults' willingness to share their personal and health information when adopting healthcare technology and services. *International Journal of Medical Informatics*, vol. 126(February), pp. 86–94.

Kim, Y. (2017). Fostering scientists' data sharing behaviors via data repositories, journal supplements, and personal communication methods. *Information Processing and Management*, vol. 53(4), pp. 871–885.

Kirkham, T., Winfield, S., Ravet, S. & Kellomäki, S. (2013). The personal data store approach to personal data security. *IEEE Security & Privacy*. IEEE, vol. 11(5), pp. 12–19.

Kitchenham, B. & Charters, S. (2007). Guidelines for performing systematic literature reviews in software engineering. EBSE Technical Report EBSE-2007-012007.

Klein, E. L. & Heines, J. M. (2013). Visualization of privacy filters for sharing sensor-based health data. *In 2013 IEEE International Conference on Healthcare Informatics*. Philadelphia, PA, USA: IEEE, p. 481.

Kolter, J., Netter, M. & Pernul, G. (2010). Visualizing past personal data disclosures. *In 2010 International Conference on Availability, Reliability and Security*. Krakow, Poland: IEEE, pp. 131–139.

Kong, Q. J., Wang, X. H. & Zhang, J. (2011). The (P, α, K) anonymity model for privacy protection of personal information in the social networks. *In 2011 6th IEEE Joint International Information Technology and Artificial Intelligence Conference*. Chongqing, China: IEEE, pp. 420–423.

KPMG. (2015). *Framing a winning data monetization strategy*. *KPMG International Cooperative*. 132669e-G.

Kuehn, A. (2013). Cookies versus clams: clashing tracking technologies and online privacy. *Info*, vol. 15(6), pp. 19–31.

Kurtz, C., Wittner, F., Semmann, M., Schulz, W. & Böhmann, T. (2019). The unlikely siblings in the GDPR family: a techno-legal analysis of major platforms in the diffusion of personal data in service ecosystems. *In 52nd Hawaii International Conference on System Sciences (HICSS)*. Maui, Hawaii, United States: Hawaii International Conference on System Sciences (HICSS), pp. 5059–5068.

Ladhari, R. & Tchetgna, N. M. (2015). The influence of personal values on Fair Trade consumption. *Journal of Cleaner Production*, vol. 87(1), pp. 469–477.

Li, W., Nirei, M. & Yamana, K. (2019). Value of data : there 's no such thing as a free lunch in the digital economy. *U.S. Bureau of Economic Analysis Working Papers*, pp. 1–48 [online].Available at: https://www.bea.gov/research/papers/2018/value-data-theres-no-such-thing-free-lunch-digital-economy.

Li, Y. (2017). Research on personal information security on social network in big data era. *In 2017 International Conference on Smart Grid and Electrical Automation (ICSGEA)*. Changsha, China: IEEE, pp. 676–678.

Li, Y., Guo, L., Wu, C., Lee, C. H. & Guo, Y. (2014). Building a cloud-based platform for personal health sensor data management. *In IEEE-EMBS International Conference on Biomedical and Health Informatics (BHI)*. Valencia, Spain: IEEE, pp. 223–226.

Liljander, V., Gummerus, J., Söderlund, M., Liljander, V. & Gummerus, J. (2015). Young consumers ' responses to suspected covert and overt blog marketing. *Internet Research*, vol. 25(4), pp. 610–632.

Lim, J. H., Kim, I. K., Bae, S. & Lee, S. H. (2014). System proposal and CRS model design applying personal Information protection for big data analysis. *In 2014 International Conference on Big Data and Smart Computing (BIGCOMP)*. Bangkok, Thailand: IEEE, pp. 231–234.

Linton, H., Kwortnik, R. J., Linton, H. & Kwortnik, R. J. (2019). Mobile usage in travel : bridging the supplier-user gap. *International Journal of Contemporary Hospitality Management*, vol. 31(2), pp. 771–789.

Logicalis. (2016). The age of digital enlightenment. United Kingdom: Logicalis Group, p. 10 [online]. [Accessed 18 April 2019]. Available at: http://www.uk.logicalis.com/globalassets/united-kingdom/microsites/real-time-generation/realtime-generation-2016-report.pdf.

Lusoli, W. & Compañó, R. (2010). From security versus privacy to identity: An emerging concept for policy design? *Info*, vol. 12(6), pp. 80–94.

Malgieri, G. (2018). 'User-provided personal content' in the EU: digital currency between data protection and intellectual property. *International Review of Law, Computers and Technology*. Taylor & Francis, vol. 32(1), pp. 118–140.

Malgieri, G. & Custers, B. (2018). Pricing privacy – the right to know the value of your personal data. *Computer Law and Security Review*, vol. 34(2), pp. 289–303.

Margarida Barreto, A. (2013). Do users look at banner ads on Facebook? *Journal of Research in Interactive Marketing*, vol. 7(2), pp. 119–139.

Mark Lee, S. H. (2016). When are frugal consumers not frugal? the influence of personal networks. *Journal of Retailing and Consumer Services*, vol. 30, pp. 1–7.

Martínez, M. A., Lasheras, J., Fernández-Medina, E., Toval, A. & Piattini, M. (2010). A personal data audit method through requirements engineering. *Computer Standards and Interfaces*, vol. 32(4), pp. 166–178.

Mei, B., Cheng, X., Xing, X., Zhang, B. & Cheng, W. (2018). Personal information prediction based on movie rating data. *In 2016 International Conference on Identification, Information and Knowledge in the Internet of Things (IIKI)*. Beijing, China: IEEE, pp. 99–103.

Mishra, B., White, S., Hosseini, D. & Arianpour, A. (2015). Storage, retrieval, analysis, pricing, and marketing of personal health care data using social networks, expert networks, and markets. US: U.S. Patent Application [online].Available at: https://patents.google.com/patent/US20150154646A1/en.

Moiso, C. & Minerva, R. (2012). Towards a user-centric personal data ecosystem the role of the bank of individuals' data. *In 2012 16th International Conference on Intelligence in Next Generation Networks*. Berlin, Germany: IEEE, pp. 202–209.

Mojžiš, J. & Laclavík, M. (2016). Accuracy of person identification based on public available data. *In 2016 IEEE 14th International Symposium on Applied Machine Intelligence and Informatics (SAMI)*. Herlany, Slovakia: IEEE, pp. 253–256.

Murray-Rust, D., O'Hara, K., Oswald, M., Kleek, M. Van & Shadbolt, N. (2015). Privacy by obfuscation with personal data management architectures: possibilities and constraints. *Workshop on the Economics of Surveillance, ACM Web Science Conference 2015*. United Kingdom, p. 6.

Murray, M. (2017). Paying for privacy and the personal data economy. *Columbia Law Review*, vol. 117(1), pp. 1–66.

Najjar, M. S. & Kettinger, W. J. (2013). Data monetization: lessons from a retailer's journey. *MIS Q. Exec.*, vol. 12(4), p. 12.

Nakagawa, Y., Matsuda, Y. & Ogi, T. (2013). Framework for handling personal data proposed system of the self-control on buying information. *In 8th International Conference*

for Internet Technology and Secured Transactions (ICITST-2013). London, UK: IEEE, pp. 107–112.

Nguyen, B. & Simkin, L. (2017). Misuse of information and privacy issues: understanding the drivers for perceptions of unfairness. *The Bottom Line*, vol. 30(2), pp. 132–150.

Norta, A., Hawthorne, D. & Engel, S. L. (2018). A privacy-protecting data-exchange wallet with ownership- and monetization capabilities. *In 2018 International Joint Conference on Neural Networks (IJCNN)*. Rio de Janeiro, Brazil: IEEE, pp. 1–8.

Oh, H., Park, S., Lee, G. M., Heo, H. & Choi, J. K. (2019). Personal data trading scheme for data brokers in IoT data marketplaces. *IEEE Access*. IEEE, vol. 7, pp. 40120–40132.

Osothongs, A. & Sonehara, N. (2014). A proposal of personal information trading platform (PIT): a fair trading between personal information and incentives. *In 2014 Fourth International Conference on Digital Information and Communication Technology and its Applications (DICTAP)*. Bangkok, Thailand: IEEE, pp. 269–274.

Osothongs, A., Suppakitpaisarn, V. & Sonehara, N. (2015). A proposed method for personal attributes disclosure valuation: a study on personal attributes disclosure in Thailand. *In 2015 7th International Conference on Information Technology and Electrical Engineering (ICITEE)*. Chiang Mai, Thailand: IEEE, pp. 408–413.

Otsuki, M. & Sonehara, N. (2013). Estimating the value of personal information with SNS utility. *I2013 International Conference on Availability, Reliability and Security*. Regensburg, Germany: IEEE, pp. 512–516.

Owusu-frimpong, N. (2008). An evaluation of customers ' perception and usage of rural community banks (RCBs) in Ghana. *International Journal of Emerging Markets*, vol. 3(2), pp. 181–196.

Parra-Arnau, J. (2018). Optimized, direct sale of privacy in personal data marketplaces. *Information Sciences*, vol. 424, pp. 354–384.

Plantin, J. C., Lagoze, C., Edwards, P. N. & Sandvig, C. (2018). Infrastructure studies meet platform studies in the age of Google and Facebook. *New Media and Society*, vol. 20(1), pp. 293–310.

Plastiras, P. & O'Sullivan, D. (2018). Exchanging personal health data with electronic health records: a standardized information model for patient generated health data and observations of daily living. *International Journal of Medical Informatics*, vol. 120(October), pp. 116–125.

Ponemon. (2015). Privacy and security in a connected life: a study of US, European and Japanese consumers. *Trend Micro Inc.* Ponemon Institute.

Portilla, I. (2018). Privacy concerns about information sharing as trade-off for personalized news. *El Profesional de la Información*, vol. 27(1), pp. 19–26.

Prentice, C., Chen, J. & Wang, X. (2019). The influence of product and personal attributes on organic food marketing. *Journal of Retailing and Consumer Services*, vol. 46, pp. 70–78.

Rapp, A. & Cena, F. (2016). Personal informatics for everyday life: how users without prior self-tracking experience engage with personal data. *International Journal of Human Computer Studies*, vol. 94, pp. 1–17.

Ravoniarison, A. & Benito, C. (2019). Mobile games: players' experiences with in-app purchases. *Journal of Research in Interactive Marketing*, vol. 13(1), pp. 62–78.

Regidor, E. (2004). The use of personal data from medical records and biological materials:

Ethical perspectives and the basis for legal restrictions in health research. *Social Science and Medicine*, vol. 59(9), pp. 1975–1984.

Rishi, M. & Gaur, S. S. (2012). Emerging sales and marketing challenges in the global hospitality industry: a thematic analysis of customer reviews from the world's top two tourist destinations. *Worldwide Hospitality and Tourism Themes*, vol. 4(2), pp. 131–149.

Rivera, M., Croes, R. & Zhong, Y. (2016). Developing mobile services: a look at first-time and repeat visitors in a small island destination. *International Journal of Contemporary Hospitality Management*, vol. 28(12), pp. 2721–2747 [online].Available at: https://doi.org/10.1108/ IJCHM-02-2015-0052.

Romualdo-Suzuki, L. C. (2015). *Data as Infrastructure for Smart Cities*. PhD Thesis. University College London.

Rousseaux, F. & Saurel, P. (2016). In light of the legal debate over personal data privacy at a time of globalized big data: making big data researchers cooperating with lawmakers to find solutions for the future. *In 2016 Intl IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld)*. Toulouse, France: IEEE, pp. 398–403.

Sánchez-Cabrero, R., Barrientos-Fernández, A., Arigita-García, A., Mañoso-Pacheco, L. & Costa-Román, O. (2018). Demographic data, habits of use and personal impression of the first generation of users of virtual reality viewers in Spain. *Data in Brief*, vol. 21, pp. 2651–2657.

Sanchez-Reillo, R., Ortega-Fernandez, I., Ponce-Hernandez, W. & Quiros-Sandoval, H. C. (2017). How to implement EU data protection regulation for R&D on personal data. *In 2017 International Carnahan Conference on Security Technology (ICCST)*. Madrid, Spain: IEEE, pp. 1–7.

Sangani, K. (2010). Who owns... your personal data? [consumer tech ownership]. *Engineering & Technology*. IEEE, vol. 5(11), pp. 28–29.

Schudy, S. & Utikal, V. (2017). 'You must not know about me'— on the willingness to share personal data. *Journal of Economic Behavior and Organization*, vol. 141, pp. 1–13.

Scott, E. M. (2013). Protecting consumer data while allowing the web to develop self-sustaining architecture: is a trans-atlantic browser-based opt-in for behavioral tracking the right solution? *Pacific McGeorge Global Business & Development Law Journal*, vol. 26(1), pp. 285–313.

Serrano, M. J. H., Greenhill, A. & Graham, G. (2015). Transforming the news value chain in the social era: a community perspective. *Supply Chain Management*, vol. 20(3), pp. 313–326.

Shrier, D., Wu, W. & Pentland, A. (2016). Blockchain & Infrastructure. *MIT Connection Science*, pp. 1–18.

Sicari, S., Rizzardi, A., Grieco, L. A. & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of things: the road ahead. *Computer Networks*, vol. 76, pp. 146–164.

Simon, J. P. (2016). User generated content – users , community of users and firms : toward new sources of co-innovation ? *info*, vol. 18(6), pp. 4–25.

Sinn, D., Kim, S. & Syn, S. Y. (2019). Information activities within information horizons: a case for college students' personal information management. *Library and Information Science Research*, vol. 41(1), pp. 19–30.

Skendzic, A., Kovacic, B. & Tijan, E. (2018). General data protection regulation - Protection

of personal data in an organisation. *In 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*. Opatija, Croatia: IEEE, pp. 1370–1375.

Smailovic, V., Galetic, V. & Podobnik, V. (2013). Implicit social networking for mobile users: Data monetization for telcos through context-aware services. *In Proceedings of the 12th International Conference on Telecommunications*. Zagreb, Croatia: IEEE, pp. 163–170.

Spiekermann, S., Böhme, R., Acquisti, A. & Hui, K.-L. (2015). Personal data markets. *Electronic Markets*, vol. 25(2), pp. 91–93.

Štitilis, D. & Laurinaitis, M. (2017). Treatment of biometrically processed personal data: problem of uniform practice under EU personal data protection law. *Computer Law and Security Review*, vol. 33(5), pp. 618–628.

Tago, K., Takagi, K., Ito, K. & Jin, Q. (2018). Specifying latent factors with a domain model for personal data analysis. *In 2018 IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing, 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTe*. Athens, Greece: IEEE, pp. 292–299.

Tallon, P., Wixom, B. H. & Buff, A. (2015). Partnering for Data Monetization Success. *Business Intelligence Journal*, vol. 20(3), pp. 28–33 [online].Available at: http://search.ebscohost.com/login.aspx?direct=true&db=plh&AN=109514949&site=eds-live.

Tett, Gi. (2018). *Should Amazon and Google pay us for our data? Financial Times* [online]. [Accessed 10 March 2019]. Available at: https://www.ft.com/content/5f023c76-c11d-11e8-8d55-54197280d3f7.

Tikkinen-Piri, C., Rohunen, A. & Markkula, J. (2018). EU general data protection regulation: changes and implications for personal data collecting companies. *Computer Law and Security Review*, vol. 34(1), pp. 134–153.

Törngren, O. (2017). Mergers in big data-driven markets - is the dimension of privacy and protection of personal data something to consider in the merger review? Thesis in EU law, Stockholm University.

Torre, I., Adorni, G., Koceva, F. & Sanchez, O. (2016). Preventing Disclosure of Personal Data in IoT Networks. *In 2016 12th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS)*. Naples, Italy: IEEE, pp. 389–396.

Torre, I., Koceva, F., Sanchez, O. R. & Adorni, G. (2016). A framework for personal data protection in the IoT. *In 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*. Barcelona, Spain: IEEE, pp. 384–391.

Tracol, X. (2015). Back to basics: the European Court of Justice further defined the concept of personal data and the scope of the right of data subjects to access it. *Computer Law and Security Review*, vol. 31(1), pp. 112–119.

Tudoran, A. A. (2019). Why do internet consumers block ads? new evidence from consumer opinion mining and sentiment analysis. *Internet Research*, vol. 29(1), pp. 144–166.

Vatavu, R. D. (2017). Smart-Pockets: body-deictic gestures for fast access to personal data during ambient interactions. *International Journal of Human Computer Studies*, vol. 103(July 2016), pp. 1–21.

Vescovi, M., Moiso, C., Antonelli, F., Pasolli, M. & Perentis, C. (2015). Building an eco-system of trusted services through user transparency, control and awareness on personal data privacy. *Procs. W3C Workshop on Privacy and User–Centric Controls*, pp. 1–6.

Vianna, D., Yong, A. M., Xia, C., Marian, A. & Nguyen, T. (2014). A tool for personal data extraction. *In 2014 IEEE 30th International Conference on Data Engineering Workshops*. Chicago, IL, USA: IEEE, pp. 80–83.

Vinodhini, A. N. & Ayyasamy, S. (2017). Prevention of personal data in cloud computing using bio-metric. *IEEE International Conference on Innovations in Green Energy and Healthcare Technologies - 2017, IGEHT 2017*, pp. 1–6.

Vishik, Svetlana, C. & Suryanarayana, L. (2011). System and method of using personal data. US: U.S. Patent.

Walker, C. & Alrehamy, H. (2015). Personal Data Lake with Data Gravity Pull. *In 2015 IEEE Fifth International Conference on Big Data and Cloud Computing*. Dalian, China: IEEE, pp. 160–167.

Wang, C. (2018). Research on the protection of personal privacy of tourism consumers in the era of big data. *In 2018 International Symposium on Computer, Consumer and Control (IS3C)*. Taichung, Taiwan: IEEE, pp. 428–431.

Wang, X. F. & Tang, H. (2012). Privacy protection in sharing personal genome sequencing data. *In 2012 IEEE Second International Conference on Healthcare Informatics, Imaging and Systems Biology*. San Diego, CA, USA: IEEE, p. 143.

Wang, Z. & Yu, Q. (2015). Privacy trust crisis of personal data in China in the era of big data: the survey and countermeasures. *Computer Law and Security Review*, vol. 31(6), pp. 782–792.

Widjaja, A. E., Chen, J. V., Sukoco, B. M. & Ha, Q. A. (2019). Understanding users' willingness to put their personal information on the personal cloud-based storage applications: an empirical study. *Computers in Human Behavior*, vol. 91, pp. 167–185.

Wilberg, J., Triep, I., Hollauer, C. & Omer, M. (2017). Big data in product development: need for a data strategy. *In 2017 Portland International Conference on Management of Engineering and Technology (PICMET)*. Portland, OR, USA: IEEE, pp. 1–10.

Woerner, S. L. & Wixom, B. H. (2015). Big data: extending the business strategy toolbox. *Journal of Information Technology*. Nature Publishing Group, vol. 30(1), pp. 60–62.

Wood, A., Shpilrain, V., Najarian, K. & Kahrobaei, D. (2019). Private naive bayes classification of personal biomedical data: application in cancer data analysis. *Computers in Biology and Medicine*, vol. 105(June 2018), pp. 144–150.

Wu, X. & Gereffi, G. (2018). Chapter 13 Amazon and Alibaba: internet governance, business models, and internationalization strategies. *International Business Research*. International Business in the Information and Digital Age, vol. 13, pp. 327–356.

Wu, Y. (2014). Protecting personal data in e-government: a cross-country study. *Government Information Quarterly*, vol. 31(1), pp. 150–159.

Xiong, L. (2015). Harnessing personal data from Internet of Things: privacy enhancing dynamic information monitoring. *In 2015 International Conference on Collaboration Technologies and Systems (CTS)*. Atlanta, GA, USA: IEEE, p. 37.

Yavuz, R. & Toker, A. (2014). Location sharing on social networks: implications for marketing. *Marketing Intelligence and Planning*, vol. 32(5), pp. 567–585.

Zajc, M. (2015). The social media dispositive and monetization of user-generated content. *Information Society*, vol. 31(1), pp. 61–67.

Zhao, Y., Wang, Z., Zou, L., Wang, J. & Hao, Y. (2014). A linked data based personal

service data collection and semantics unification method. *In 2014 International Conference on Service Sciences*. Wuxi, China: IEEE, pp. 118–123.

Zharova, A. K. & Elin, V. M. (2017). The use of big data: a Russian perspective of personal data security. *Computer Law and Security Review*, vol. 33(4), pp. 482–501.

Zheng, X., Mukkamala, R. R., Vatrapu, R. & Ordieres-Mere, J. (2018). Blockchain-based personal health data sharing system using cloud storage. *In 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom)*. Ostrava, Czech Republic: IEEE, p. 6.

Zhihan, L., Quan, Y. & Lu, L. (2016). Decentralized mobile SNS architecture and its personal information management mechanism. *China Communications*. China Institute of Communications, vol. 13(2), pp. 189–199.

Zhong, M. & Liu, M. (2009). A flexible data warehousing approach for one-stop querying on heterogeneous personal information. *In 2009 20th International Workshop on Database and Expert Systems Application*. Linz, Austria: IEEE, pp. 412–416.

Zou, H. (2016). Protection of personal information security in the age of big data. *In 2016 12th International Conference on Computational Intelligence and Security (CIS)*. Wuxi, China: IEEE, pp. 586–589.

Zyskind, G., Nathan, O. & Pentland, A. 'Sandy'. (2015). Decentralizing privacy: using blockchain to protect personal data. *In 2015 IEEE Security and Privacy Workshops*. San Jose, CA, USA: IEEE, pp. 180–184.

Appendices

Appendix A: Quality Assessment Results

Article	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Total	Percentage
A1	1	1	1	0	0	1	1	1	0	1	7	70%
A2	1	1	0	0	0	1	1	0	0	1	5	50%
A3	1	1	0	0	1	1	1	0	1	1	7	70%
A4	1	0	0	0	1	0	1	0	1	1	5	50%
A5	1	0	0	0	1	0	0	0	1	1	4	40%
A6	0	1	1	0	1	1	1	0	1	0	6	60%
A7	1	0	1	0	1	1	1	0	1	1	7	70%
A8	0	1	1	0	0	1	0	0	0	0	3	30%
A9	0	0	0	0	1	0	0	0	0	1	2	20%
A10	1	0	0	0	1	1	1	1	0	1	6	60%
A11	1	0	0	0	0.5	1	1	0	0	0	3.5	35%
A12	0	0	1	0	0.5	1	0	0	0	1	3.5	35%
A13	1	1	0	0	0	1	1	0	1	0	5	50%
A14	0	0	0	0	1	1	0	0	0	1	3	30%
A15	0	0	0	0	0	0	0	0	0	1	1	10%
A16	0	0	0	0	1	0	0	0	0	1	2	20%
A17	0	1	1	0	0.5	0	1	0	1	1	5.5	55%
A18	0	0	0	0	0	0	0	0	0	0	0	0%
A19	0	0	1	0	1	1	0	0	0	1	4	40%
A20	0	0	0	0	1	1	0	0	1	1	4	40%
A21	0	0	0	0	0	0	0	0	0	1	1	10%
A22	0	0	1	1	1	0.5	1	0	1	1	6.5	65%
A23	0	0.5	0	0	0	0	0	0	1	0	1.5	15%
A24	1	0	1	0	1	0	0	0	0	1	4	40%
A25	0	0	1	0	0	0	0	0	0	1	2	20%
A26	0	0	1	0	0	0	0	1	0	1	3	30%
A27	0	0	1	0	0	1	0	0	0	0	2	20%
A28	0	0	0	0	1	0	0	0	0	0	1	10%
A29	0	1	1	0	1	1	1	0	0	1	6	60%
A30	0.5	0	1	0	1	1	1	0	1	1	6.5	65%
A31	1	0	0	0	1	1	0	0	1	1	5	50%
A32	0.5	0	0	0	1	0.5	0	0	0	0	2	20%
A33	0.5	1	1	0	1	0	1	1	0	1	6.5	65%
A34	0	1	1	1	0	1	1	0	0	1	6	60%
A35	0.5	0	0	0	1	0.5	0	1	0	1	4	40%
A36	0	0.5	0	0	0	0.5	0.5	0	0	0	1.5	15%
A37	0	0	0	0	1	0	1	0	0	0	2	20%

A38	0.5	1	1	0	0.5	1	1	1	0	1	7	70%
A39	0	0	1	0	0	1	0	0	0	1	3	30%
A40	1	1	0	0	0	1	0	1	0	1	5	50%
A41	1	1	1	0	0	1	1	0	1	1	7	70%
A42	0	0	0	0	1	0.5	0.5	0	1	1	4	40%
A43	1	1	0	1	0	0.5	1	0	1	1	6.5	65%
A44	0.5	1	0	0	1	0.5	0	1	0	0	4	40%
A45	0.5	1	0	0	1	0	0	0	0	1	3.5	35%
A46	1	1	0	0	1	0.5	0	0	0	1	4.5	45%
A47	0	0	1	0	0	0	0	0	0	0	1	10%
A48	0	0	1	0	0	0.5	0	0	1	0	2.5	25%
A49	0	1	0.5	0	0	0	0	0	0	1	2.5	25%
A50	1	0	0	0	0	1	0	0	0	0	2	20%
A51	0	1	0.5	0	1	1	1	1	1	1	7.5	75%
A52	0	0	0	0	0	0.5	0.5	0	0	1	2	20%
A53	0	1	0	0	0	1	0	0	1	1	4	40%
A54	1	0.5	1	0	1	1	1	0	0	1	6.5	65%
A55	0	0	0	0	0	0.5	0	0	0	0	0.5	5%
A56	0	0	0	0	1	0.5	0	0	0	0	1.5	15%
A57	0	1	0	0	1	1	0	0	0	1	4	40%
A58	1	0	1	0	0	0	0	0	1	0	3	30%
A59	1	0	1	0	1	1	0	0	1	0	5	50%
A60	1	1	1	0	1	1	0	0	0	0	5	50%
A61	0	1	0	0	0.5	0	0	1	1	1	4.5	45%
A62	0	0	0	0	1	0.5	0	1	0	1	3.5	35%
A63	1	0	1	0	1	0	0	0	1	1	5	50%
A64	1	0	0.5	0	1	0.5	1	1	0	1	6	60%
A65	1	0	1	0	0.5	0	0	1	0	0	3.5	35%
A66	0	0	0	0	1	0	0	0	0	0	1	10%
A67	0	0	0	0	1	1	0	1	1	1	5	50%
A68	1	0	0	0	1	1	0	0	1	0	4	40%
A69	0	0	0	0	0	1	0	0	1	0	2	20%
A70	1	0	0	0	1	0.5	0	1	1	1	5.5	55%
A71	1	0	0	0	0	0	0	0	0	0	1	10%
A72	0	0	1	0	1	0	0	0	0	1	3	30%
A73	0.5	0	0	0	0	0.5	0	0	1	1	3	30%
A74	0.5	0	0	0	0	0.5	0	0	1	0	2	20%
A75	0.5	0	0	0	0.5	0.5	1	0	0	0	2.5	25%
A76	0.5	0	0	0	1	0	0	1	1	0	3.5	35%
A77	1	0	1	0	0.5	0.5	0	0	0	1	4	40%
A78	1	0	1	0	1	0	0	1	0	1	5	50%
A79	1	0	0	0	1	0.5	1	0	1	1	5.5	55%

A80	0	0	1	0	0.5	0.5	0	0	0	0	2	20%
A81	0.5	0	0	0	1	0.5	0	1	0	1	4	40%
A82	1	0	1	0	1	0.5	0	1	1	0	5.5	55%
A83	0	0	0.5	0	0	0.5	0	0	1	0	2	20%
A84	0.5	0	0	0	0.5	1	0	1	0	0	3	30%
A85	0	0	1	0	0.5	1	0	0	1	1	4.5	45%
A86	0	0	0	0	1	1	0	0	0	0	2	20%
A87	0	1	0	0	0.5	0.5	0	0	1	0	3	30%
A88	0	0	1	0	1	0	0	0	0	1	3	30%
A89	1	0.5	0	0	0	0	0	0	0	0	1.5	15%
A90	0	0	0	0	0.5	0	0	0	0	0	0.5	5%
A91	1	0	0	0	1	1	1	0	1	1	6	60%
A92	0	1	0	0	1	0	0	0	1	1	4	40%
A93	1	0	0	1	1	1	0	1	0	1	6	60%
A94	0.5	0.5	0	0.5	1	1	1	1	1	1	7.5	75%
A95	0.5	0	0	0	0.5	0.5	0	0	0	0	1.5	15%
A96	0	0.5	0	0	0.5	0	0	0	1	0	2	20%
A97	0	0	0	0	0	0	0	1	0	0	1	10%
A98	0.5	0	0	0	1	0	1	0	1	0	3.5	35%
A99	0.5	0.5	0	0	0.5	0.5	0	0	0	0	2	20%
A100	0	0	1	0	0	0	0	0	1	0	2	20%
A101	0	0	0	0	1	0.5	0	0	1	0	2.5	25%
A102	1	0	0.5	0	0.5	0	0.5	0	1	1	4.5	45%
A103	0	0	0	0	0	1	0	0	0	0	1	10%
A104	0	0	0	0	1	1	0	1	0	0	3	30%
A105	0	0	0	0	0.5	0	0	0	0	0	0.5	5%
A106	1	0	0	0	0.5	0.5	0	1	0	0	3	30%
A107	1	0	1	0	0	1	1	0	1	1	6	60%
A108	1	0	0	0	0	1	1	1	1	0	5	50%
A109	0.5	0	0	0	0	1	1	0	0	1	3.5	35%
A110	0	1	0	0	0	0	1	0	1	1	4	40%
A111	0	1	1	1	0	0	1	0	1	1	6	60%
A112	1	0	0	0	0	1	1	0	1	0	4	40%
A113	0.5	0	1	0	0	1	1	0	1	1	5.5	55%
A114	0	0	1	0	0	0	0	0	0	1	2	20%
A115	1	0	1	0	0	0	1	0	1	1	5	50%
A116	1	0	0	0	0.5	1	1	0	1	1	5.5	55%
A117	1	0	0	0	0	0	0	0	0	0	1	10%
A118	1	1	1	0.5	0	1	1	0	1	1	7.5	75%
A119	1	0	0	0	0	1	0	0	1	0	3	30%
A120	0	0	0	0	0	0	1	0	1	1	3	30%
A121	1	0	0	0	0	0.5	1	0	1	1	4.5	45%

A122	1	0	0	0	0	0	0.5	0	0	1	2.5	25%
A123	0	0	0	0	0.5	0	0.5	0	0	0	1	10%
A124	0	0	0	0	0	0	1	0	1	0	2	20%
A125	0	0	0	0	0.5	0	1	0	0	0	1.5	15%
A126	1	0	0	0	0	0	0.5	0	1	1	3.5	35%
A127	1	0	0	0	0	0	0	0	0	1	2	20%
A128	0	0.5	0	0	0	0	0.5	0	0	1	2	20%
A129	0	0	0	0	0	1	0	0	1	0	2	20%
A130	0	0	1	0	0	0	1	0	1	0	3	30%
A131	1	0	0	0	0	0	0	0	0	1	2	20%
A132	0	0	0	1	0	0	0	0	0	0	1	10%
A133	1	0	0	0	0	0	1	0	0	1	3	30%
A134	1	0	0	0	0	0	0	0	0	1	2	20%
A135	0	0.5	0	0	0	0	0	0	0	0	0.5	5%
A136	0.5	0	0	0	0	0	0	0	0	0	0.5	5%
A137	1	0	1	0	0	0.5	0	0	0	0	2.5	25%
A138	1	0	0	0	0	0	1	0	0	1	3	30%
A139	1	0	0	1	0.5	0.5	0.5	0	1	0	4.5	45%
A140	1	0	0	0	0	1	1	0	0	0	3	30%
A141	0	1	0	0	0	0.5	1	0	1	1	4.5	45%
A142	1	0	0	0	1	0.5	1	0	1	0	4.5	45%
A143	1	0	1	0	1	0.5	1	0	0	1	5.5	55%
A144	0	0	1	0	1	1	1	0	0	1	5	50%
A145	0	0	0	0	0.5	0.5	0	0	0	0	1	10%
A146	0	0	0.5	0	0.5	0	0	0	0	0	1	10%
A147	0	0	0	0	0	0.5	0	0	1	0	1.5	15%
A148	0	0	1	0	1	0	1	0	0	1	4	40%
A149	0.5	0	1	1	1	0.5	1	0	1	1	7	70%
A150	0	0	0	0	0	0	0	0	1	1	2	20%
A151	1	0	1	0	1	0.5	1	0	0	0	4.5	45%
A152	0	0	0	0	1	0.5	0	0	0	1	2.5	25%
A153	1	0	1	0	0.5	0.5	0	0	0	1	4	40%
A154	1	0	0	0	0	1	1	0	0	0	3	30%
A155	0	0	0	0	1	0	1	0	0	1	3	30%
A156	0	0	0	0	1	0	0	0	1	0	2	20%
A157	0	0	1	0	0	0	1	0	0	0	2	20%
A158	0.5	0	1	0	0	1	1	0	1	0	4.5	45%
A159	0	0	0	0	0	1	0	0	0	1	2	20%
A160	0	0	0	0	0.5	0	0	0	0	0	0.5	5%
A161	0	0	1	0	1	1	0	0	0	1	4	40%
A162	0.5	0	0	0	1	1	1	0	0	0	3.5	35%
A163	0	0	0	0	1	0	1	0	1	1	4	40%

A164	0	0	0	0	0	0	1	0	0	0	1	10%
A165	0	0	1	0	1	0.5	1	0	1	0	4.5	45%
A166	0	0.5	1	0	0.5	1	1	0	0	1	5	50%
A167	0	1	0	0	0.5	0	0	0	1	1	3.5	35%
A168	0	0	1	0	0	0	0	0	1	1	3	30%
A169	1	0	1	0	0.5	0.5	0	0	0	1	4	40%
A170	0	1	0	0	1	0.5	0	0	0	0	2.5	25%
A171	1	0	0	0	1	0	0	0	0	1	3	30%
A172	1	1	0.5	0	1	1	0	0	0	1	5.5	55%
A173	1	0	1	0	0	0.5	0.5	0	0	0	3	30%
A174	0	0	0	0	0	0	0	0	0	0	0	0%
A175	0	0	0	0	0	0	0	0	0	0	0	0%
A176	0	0	0	0	0	0.5	0	0	0	0	0.5	5%
A177	1	0	0	0	1	0	1	0	0	1	4	40%
A178	0	0	0	0	1	0	1	1	0	0	3	30%
A179	0	0	0	0	0	0.5	0	1	0	1	2.5	25%
A180	0	0	0.5	0	1	0.5	1	0	0	1	4	40%
A181	0	0.5	0	0	0	0	1	0	1	1	3.5	35%
A182	1	1	1	0	1	0	1	1	1	1	8	80%

Appendix B: IEEE Studies Collection

IEEE impact factor	impact factor	Ranking	Conference	Journal Name	Paper title	year	citations
		A	2018 International Joint Conference on Neural Networks (IJCNN)		A Privacy-Protecting Data-Exchange Wallet with Ownership- and Monetization Capabilities	2018	1
		B	2015 2nd International Conference on Information Science and Security (ICISS)		Monetization of Personal Identity Information: Technological and Regulatory Framework	2015	1
			2018 IEEE Games, Entertainment, Media Conference (GEM)		Data Privacy, Transparency and the Data-Driven Transformation of Games to Services	2018	0
			2014 2nd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering		Explaining the Role of Trust in Cloud Service Acquisition	2014	5
			2014 International Conference on Service Sciences		A Linked Data Based Personal Service Data Collection and Semantics Unification Method	2014	0
			2012 16th International Conference on Intelligence in Next Generation Networks		Towards a user-centric personal data ecosystem The role of the bank of individuals' data	2012	24
			2009 20th International Workshop on Database and Expert Systems Application		A Flexible Data Warehousing Approach for One-Stop Querying on Heterogeneous Personal Information	2009	1
		UIC: B ATC: C	2016 Intl IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld)		In Light of the Legal Debate over Personal Data Privacy at a Time of Globalized Big Data: Making Big Data Researchers Cooperating with Lawmakers to Find Solutions for the Future	2016	0
	3.557			IEEE Access	A Data-Driven Security Risk Assessment Scheme for Personal Data Protection	2018	1
		C	5th IEEE/ACIS International Conference on Computer and Information Science and 1st IEEE/ACIS International Workshop on Component-Based Software Engineering,Software Architecture and Reuse (ICIS-COMSAR'06)		Application Services Based on Personal Data Ontology	2006	3
	1.239			IEEE Security & Privacy	The Personal Data Store Approach to Personal Data Security	2013	13
		C	2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom)		Blockchain-based Personal Health Data Sharing System Using Cloud Storage	2018	2
		C	2016 13th International Conference on Embedded Software and Systems (ICESS)		DSPM: A Platform for Personal Data Share and Privacy Protect Based on Metadata	2016	1
		C	2016 14th Annual Conference on Privacy, Security and Trust (PST)		Effective frameworks for delivering compliance with personal data privacy regulatory requirements	2016	3
			2015 IEEE Fifth International Conference on Big Data and Cloud Computing		Personal Data Lake with Data Gravity Pull	2015	26
			2018 International Symposium on Computer, Consumer and Control (IS3C)		Research on the Protection of Personal Privacy of Tourism Consumers in the Era of Big Data	2018	0
		C	2016 First IEEE International Conference on Computer Communication and the Internet (ICCCI)		The legal debate about personal data privacy at a time of big data mining and searching: Making big data researchers cooperating with lawmakers to find solutions for the future	2016	0
		C	2013 IEEE 14th International Conference on Mobile Data Management		Personal Data Management with Secure Hardware: How to Keep Your Data at Hand	2013	5
		TrustCom: A	2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)		Blockchain as a Notarization Service for Data Sharing with Personal Data Store	2018	0
			2017 International Conference on Engineering, Technology and Innovation (ICE/ITMC)		Big data analytics in public safety and personal security: Challenges and potential	2017	3
			2018 IEEE Conference on Big Data and Analytics (ICBDA)		Predicting Personal Mobility Data Disclosure	2018	0
			2014 International Conference on Big Data and Smart Computing (BIGCOMP)		System proposal and CRS model design applying personal Information protection for BIG DATA analysis	2014	3
		C	2018 4th International Conference on Computer and Technology Applications (ICCTA)		Personal data protection maturity model for the micro financial sector in Peru	2018	3
			2017 International Conference on Smart Grid and Electrical Automation (ICSGEA)		Research on Personal Information Security on Social Network in Big Data Era	2017	0
		C	2016 12th International Conference on Computational Intelligence and Security (CIS)		Protection of Personal Information Security in the Age of Big Data	2016	1
			2014 IEEE 30th International Conference on Data Engineering Workshops		A tool for personal data extraction	2014	8
9.107			2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)		General data protection regulation — Protection of personal data in an organisation	2018	0
			2014 Fourth International Conference on Digital Information and Communication Technology and its Applications (DICTAP)		A proposal of personal information trading platform (PIT): A fair trading between personal information and incentives	2014	7
				IEEE Access	Personal Data Trading Scheme for Data Brokers in IoT Data Marketplaces	2019	
			2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)		A framework for personal data protection in the IoT	2016	8
		DASC: C	2018 IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing, 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech)		Specifying Latent Factors with a Domain Model for Personal Data Analysis	2018	1
			2017 IST-Africa Week Conference (IST-Africa)		Are organisations in South Africa ready to comply with personal data protection or privacy legislation and regulations?	2017	2
					Do users know or care about what is done with their personal data: A South African study	2018	1
			2016 12th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS)		Preventing Disclosure of Personal Data in IoT Networks	2016	4
			2015 7th International Conference on Information Technology and Electrical Engineering (ICITEE)		A proposed method for personal attributes disclosure valuation: A study on personal attributes disclosure in Thailand	2015	2
		C	2013 IEEE 5th International Conference on Cloud Computing Technology and Science		Monitoring Personal Data Transfers in the Cloud	2013	11
			2016 International Conference on Identification, Information and Knowledge in the Internet of Things (IIKI)		Personal Information Prediction Based on Movie Rating Data	2016	0
			8th International Conference for Internet Technology and Secured Transactions (ICITST-2013)		Framework for handling personal data proposed system of the self-control on buying information	2013	2
			2011 6th IEEE Joint International Information Technology and Artificial Intelligence Conference		The (P, α, K) anonymity model for privacy protection of personal information in the social networks	2011	0
			2018 15th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON)		Investigating the Protection of Customers' Personal Data in the Ridesharing Applications: A Desk Research in Indonesia	2018	0
			2015 IEEE Security and Privacy Workshops		Decentralizing Privacy: Using Blockchain to Protect Personal Data	2015	538
			IEEE Transactions on Emerging Topics in Computing		Cyber-Enabled Well-Being Oriented Daily Living Support Based on Personal Data Analytics	2017	3
				IEEE Access	Context-Aware Scheduling in Personal Data Collection From Multiple Wearable Devices	2017	7
		C	2016 IEEE 14th International Symposium on Applied Machine Intelligence and Informatics (SAMI)		Accuracy of person identification based on public available data	2016	0
			2017 International Carnahan Conference on Security Technology (ICCST)		How to implement EU data protection regulation for R&D on personal data	2017	0
		B	2010 International Conference on Availability, Reliability and Security		Visualizing Past Personal Data Disclosures	2010	28
			2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)		GDPR and the reuse of personal data in scientific research	2018	0
			2013 IEEE International Conference on Healthcare Informatics		Visualization of Privacy Filters for Sharing Sensor-Based Health Data	2013	2
			Engineering & Technology		Who owns... Your personal data? [Consumer Tech Ownership]	2010	5
			2017 International Conference on Innovations in Green Energy and Healthcare Technologies (IGEHT)		Prevention of personal data in cloud computing using bio-metric	2017	0
			2015 Fifth International Conference on Communication Systems and Network Technologies		Study on the Legal Protection of Personal Information and its Free Movement in Electronic Commerce	2015	0
			China Communications		Decentralized mobile SNS architecture and its personal information management mechanism	2016	1
			IEEE-EMBS International Conference on Biomedical and Health Informatics (BHI)		Building a cloud-based platform for personal health sensor data management	2014	18
			2010 Seventh International Conference on Information Technology: New Generations		Personal Information Protection Model Based on Mobile Agent	2010	0
		C	Proceedings of the ITI 2011, 33rd International Conference on Information Technology Interfaces		Semantic technologies for Personal Information Management	2011	36
			2011 International Conference on User Science and Engineering (i-USEr)		Using diary to uncover users' personal information management (PIM) behaviours	2011	0

Appendix C: Emerald Insight Studies Collection

cite score		impact factor		Journal Name	Paper title	year	citations
2017	Tracker 2018	2017	5-year (2017)				
3.56	5.12	2.874	3.464	International Journal of Contemporary Hospitality Management	Mobile usage in travel: bridging the supplier-user gap	2019	0
					Developing mobile services: A look at first-time and repeat visitors in a small island destination	2016	9
					Poster child and guinea pig – insights from a structured literature review on Airbnb	2019	3
0.63	0.97			Journal of Business Strategy	The goose that laid the golden eggs: personal data and the Internet of Things	2019	0
4.08	4.70	3.414	5.407	Journal of Service Management	Customer experience challenges: bringing together digital, physical and social realms	2018	12
4.72	6.06	3.838	4.947	Internet Research	Young consumers' responses to suspected covert and overt blog marketing	2015	41
					Why do internet consumers block ads? New evidence from consumer opinion mining and sentiment analysis	2019	1
Volumes from this series are included in the Thomson Reuters Book Citation Index				Book: Studies in Law, Politics and Society	Data Reuse and the Problem of Group Identity	2017	1
1.02	1.5			info	From security versus privacy to identity: an emerging concept for policy design?	2010	7
					Cookies versus clams: clashing tracking technologies and online privacy	2013	9
					User generated content – users, community of users and firms: toward new sources of co-innovation?	2016	10
1.71	2.06			Journal of Consumer Marketing	The impact of compensation on information ownership and privacy control	2014	19
					The first decade: emerging issues of the twenty-first century in consumer marketing	2011	20
				Book Series: Progress in International Business Research	Chapter 13 Amazon and Alibaba: Internet Governance, Business Models, and Internationalization Strategies	2018	
0.90	1.47	0.759	1.014	Library Hi Tech	Towards an understanding of data work in context: Emerging issues of economy, governance, and ethics	2016	4
2.41	2.71			Journal of Research in Interactive Marketing	Consumer behavior in the online context	2014	50
					Omni-channel marketing, integrated marketing communications and consumer engagement: A research agenda	2017	27
					Mobile games: players' experiences with in-app purchases	2019	0
					Do users look at banner ads on Facebook?	2013	109
2.01	2.64	1.675	2.05	Online Information Review	Phones, privacy, and predictions: A study of phone logged data to predict privacy attitudes of individuals	2018	0
2.00	2.33	1.497	2.545	European Journal of Marketing	Moving beyond Goffman: the performativity of anonymity on SNS	2019	0
					Conceptualisations of the consumer in marketing thought	2016	11
0.61	0.75			Worldwide Hospitality and Tourism Themes	Emerging sales and marketing challenges in the global hospitality industry: A thematic analysis of customer reviews from the world's top two tourist destinations	2012	22
0.68	0.69			Strategy & Leadership	New business models for emerging media and entertainment revenue opportunities	2011	43
1.41	1.2			Information and Computer Security	Attention and past behavior, not security knowledge, modulate users' decisions to login to insecure websites	2016	4
1.71	2.44	1.421		Marketing Intelligence & Planning	Location sharing on social networks: implications for marketing	2014	13
0.77	0.47			Journal of Information, Communication and Ethics in Society	Will "smarter" marketing end social discrimination? A critical review	2013	3
1.54	2.27			International Journal of Emerging Markets	An evaluation of customers' perception and usage of rural community banks (RCBs) in Ghana	2008	44
2.46	2.81	1.395	1.444	Managing Service Quality: An International Journal	Calculating the value of customers' referrals	2003	105
1.70	2.08	1.289	1.583	British Food Journal	Information sharing and its integrative role: An empirical study of the malt barley value chain in Ethiopia	2016	1
0.31	1.44			Pacific Accounting Review	The valuation and pricing of information assets	2016	2
1.65	2.42			The TQM Journal	Success in the Relationship Age: building quality relationship assets for market value creation	2002	124
1.70	2.69			Journal of Hospitality and Tourism Technology	Online social networking: redefining the human web	2010	197
This journal is owned by Turkish Capital Markets Association & delivered by Emerald Publishing Services				Journal of capital markets studies	Understanding sustainability for socially responsible investing	2017	2
0.24	0.56			The Bottom Line	Misuse of information and privacy issues: understanding the drivers for perceptions of unfairness	2017	2

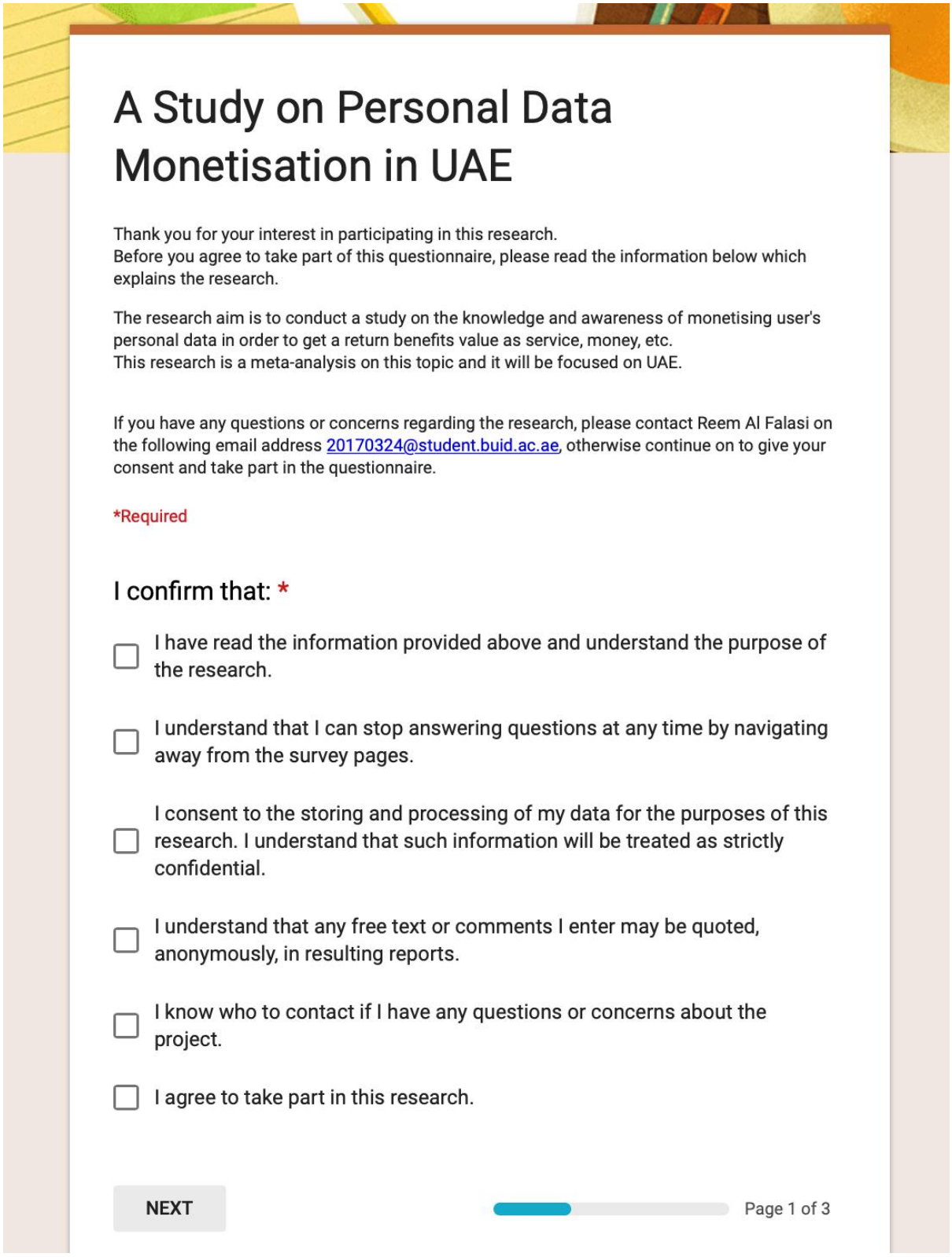
Appendix D: Science Direct Studies Collection

5-year impact factor	impact factor	citescore	Ranking (SJR)	Journal Name	Paper title	year	citations
		1.03	0.258	Procedia Computer Science	Monetizing Personal Data: A Two-Sided Market Approach	2016	2
2.439	2.551	3.76	0.805	Information Systems	Personal Data Management Systems: The security and functionality standpoint	2019	1
					Optimized, direct sale of privacy in personal data marketplaces	2018	0
1.112	0.867	0.78	0.334	Computer Law & Security Review	Pricing privacy – the right to know the value of your personal data	2018	11
					Treatment of biometrically processed personal data: Problem of uniform practice under EU personal data protection law	2017	0
					Functional anonymisation: Personal data and the data environment	2018	4
					The use of Big Data: A Russian perspective of personal data security	2017	6
					EU General Data Protection Regulation: Changes and implications for personal data collecting companies	2018	46
					Back to basics: The European Court of Justice further defined the concept of personal data and the scope of the right of data subjects to access it	2015	2
					Anonymisation of personal data – A missed opportunity for the European Commission	2014	7
					Privacy trust crisis of personal data in China in the era of Big Data: The survey and countermeasures	2015	18
2.224	2.3	3.38	0.605	International Journal of Human-Computer Studies	Personal informatics for everyday life: How users without prior self-tracking experience engage with personal data	2016	50
					Smart-Pockets: Body-deictic gestures for fast access to personal data during ambient interactions	2017	7
	4.516	8.81		International Journal of Information Management	A regulatory model for personal data on social networking services in the UK	2016	8
					Registration, access and use of personal knowledge in organizations	2018	1
4.82	4.313	3.82	1.707	The Journal of Strategic Information Systems	Handle with care: How online social network providers' privacy policies impact users' information sharing behavior	2015	46
3.378	2.957	3.56	1.247	International Journal of Medical Informatics	Personal health data: A systematic mapping study	2018	0
					Exchanging personal health data with electronic health records: A standardized information model for patient generated health data and observations of daily living	2018	0
					Donor's support tool: Enabling informed secondary use of patient's biomaterial and personal data	2017	8
					Older Adults' Willingness to Share Their Personal and Health Information When Adopting Healthcare Technology and Services	2019	0
2.14	1.296	1.69	1.583	Journal of Economic Behavior & Organization	'You must not know about me'—On the willingness to share personal data	2017	13
					Disclosure of personal information under risk of privacy shocks	2016	15
3.13	2.819	3.75	0.874	Engineering Applications of Artificial Intelligence	On the regulation of personal data distribution in online advertising platforms	2019	0
2.681	2.613	3.47	0.459	Computer Communications	Protecting personal data in IoT platform scenarios through encryption-based selective disclosure	2018	0
5.231	4.009	5.82	1.321	Government Information Quarterly	Unveiling the coverage patterns of newspapers on the personal data protection act	2017	2
					Protecting personal data in E-government: A cross-country study	2014	34
2.168	2.115	2.51	0.591	Computers in Biology and Medicine	Private naive bayes classification of personal biomedical data: Application in cancer data analysis	2019	0
2.641	3.444	4.23	0.92	Information Processing & Management	Fostering scientists' data sharing behaviors via data repositories, journal supplements, and personal communication methods	2017	5
1.479	1.465	2.08	0.378	Computer Standards & Interfaces	A Personal Data Audit Method through Requirements Engineering	2010	17
2.862	2.65	3.86	0.684	Computers & Security	CooPeD: Co-owned Personal Data management	2014	9
					Analyzing research trends in personal information privacy using topic modeling	2017	12
		0.52	0.19	Network Security	Protecting personal data from untrusted web-based data services	2011	1
					Failed firm banned from selling customers' personal data	2009	
2.39	1.967	2.28	1.181	Personality and Individual Differences	Age- and gender-related differences in the structure and the meaning of personal values	2019	0
4.417	3.536	4.57	1.555	Computers in Human Behavior	Willingness to provide personal information: Perspective of privacy calculus in IoT services	2019	1
					I trust not therefore it must be risky: Determinants of the perceived risks of disclosing personal data for e-government transactions	2011	51
					Understanding users' willingness to put their personal information on the personal cloud-based storage applications: An empirical study	2019	0
					Factors influencing willingness to provide personal information for personalized recommendations	2018	1
					Personal and social factors involved in internet addiction among adolescents: A meta-analysis	2018	4
3.835	3.007	3.38	1.91	Social Science & Medicine	The use of personal data from medical records and biological materials: ethical perspectives and the basis for legal restrictions in health research	2004	44
		0.7	0.341	Data in Brief	Demographic data, habits of use and personal impression of the first generation of users of virtual reality viewers in Spain	2018	2
2.434	2.067	2.11	1.154	Nurse Education Today	A patient as a self-manager of their personal data on health and disease with new technology – challenges for nursing education	2015	20
2.028	1.836	2.67	0.503	Journal of Visual Communication and Image Representation	Personal-location-based temporal segmentation of egocentric videos for lifelogging applications	2018	6
1.112	1.013	1.11	0.322	Health Policy and Technology	An overview of electronic personal health records	2018	0
1.886	1.372	1.7	1.188	Library & Information Science Research	Information activities within information horizons: A case for college students' personal information management	2019	
	2.919	3.56	1.216	Journal of Retailing and Consumer Services	When are frugal consumers not frugal? The influence of personal networks	2016	5
4.792	3.89	5.24	1.628	Information & Management	Impact of anonymity on roles of personal and group identities in online communities	2019	1
6.352	5.651	5.79	1.467	Journal of Cleaner Production	The influence of personal values on Fair Trade consumption	2015	46
3.21	2.85	3.07	1.787	Journal of Research in Personality	Judging personal values and personality traits: Accuracy and its relation to visibility	2016	8
	2.919	3.56	1.216	Journal of Retailing and Consumer Services	The influence of product and personal attributes on organic food marketing	2019	1

Appendix E: Google Scholar Studies Collection

SJR	5 years impact factor	impact factor	Cite score	Ranking	Publisher	Conference	Journal Name	Paper title	year	citations
					Taylor & Francis		International Journal on Media Management	Consumers' Willingness to Share Personal Data: Implications for Newspapers' Business Models	2016	23
						SPECIAL FORUM: Monetization of User-Generated Content-Marx Revisited	The Information Society	Personal Data: Blind Spot of the "Affective Law of Value"?	2015	31
								The social media dispositive and monetization of user-generated content	2015	9
							International Review of Law, Computers & Technology	'User-provided personal content' in the EU: digital currency between data protection and intellectual property	2018	2
					HeinOnline		COLUMBIA LAW REVIEW	Paying for Privacy and the Personal Data Economy	2017	23
				C	Springer	IFIP International Conference on Trust Management		Building an Eco-System of Trusted Services via User Control and Transparency on Personal Data	2015	7
					cornell university		arXiv preprint arXiv:1202.4503	A critical look at decentralized personal data architectures	2012	63
3.44	2.713	1.905	2.39		Elsevier		Journal of Public Economics	Privacy and personal data collection with information externalities	2019	5
1.247	3.378	2.957	3.56	A*			International Journal of Medical Informatics	Trustworthy reuse of health data: A transnational perspective	2013	73
0.334	1.112	0.867	0.78				Computer Law & Security Review	Pricing privacy – the right to know the value of your personal data	2018	11
1.707	4.82	4.313	3.82	A			The Journal of Strategic Information Systems	Handle with care: How online social network providers' privacy policies impact users' information sharing behavior	2015	46
0.805	2.439	2.551	3.76	A*			Information Systems	Personal Data Management Systems: the Security and Functionality Standpoint	2018	1
1.373	4.810	4.516	5.78	C			International Journal of Information Management	Exploring the economic value of personal information from firms' financial statements	2014	20
				A*	ACM -DL	Proceedings of the 22nd international conference on World Wide Web		Your browsing behavior for a big mac: Economics of personal information online	2013	102
					IEEE	Proceedings of the 12th International Conference on Telecommunications		Implicit social networking for mobile users: Data monetization for telcos through context-aware services	2013	5
				A		2017 IEEE 16th International Symposium on Network Computing and Applications (NCA)		The effect of a blockchain-supported, privacy-preserving system on disclosure of personal data	2017	3
					springer		Journal of Direct, Data and Digital Marketing Practice	The consumer data revolution: The reshaping of industry competition and a new perspective on privacy	2014	6
				A*	ACM -DL	Proceedings of the SIGCHI Conference on Human Factors in Computing Systems		"Everybody knows what you're doing": a critical design approach to personal informatics	2013	62
					Massachusetts Institute of Technology-Connection Science			Blockchain & infrastructure (identity, data security)	2016	32
					U.S. Patent Google Patents			System and method of using personal data	2011	26
								System and method for dynamic and secure communication and synchronization of personal data records	2018	1
								Storage, retrieval, analysis, pricing, and marketing of personal health care data using social networks, expert networks, and markets	2015	11
					Surveillance & Society			Personal Data Spaces: An Intervention in Surveillance Capitalism?	2017	2
					IOS Press			Digital enlightenment yearbook 2013: The value of personal data	2013	13
					ACM -DL	NetEcon '17 Proceedings of the 12th workshop on the Economics of Networks, Systems and Computation		A cooperative game-theoretic approach to quantify the value of personal data in networks	2017	4
					Accenture			Guarding and growing personal data value	2016	5
					Delft: TNO			Personal data markets	2014	4
				A	Hawaii	Proceedings of the 52nd Hawaii International Conference on System Sciences		BPDIMS: A Blockchain-based Personal Data and Identity Management System	2019	1
								The Unlikely Siblings in the GDPR Family: A Techno-Legal Analysis of Major Platforms in the Diffusion of Personal Data in Service Ecosystems	2019	1
							Master's thesis	DATA MONETIZATION – HOW AN ORGANIZATION CAN GENER- ATE REVENUE WITH DATA?	2017	1
					bof.nl		Exploring the Boundaries of Big Data	From collection to use in privacy regulation? a forward-looking comparison of european and us frameworks for personal data processing	2016	5
							JeDEM-eJournal of eDemocracy and Open Government	Tokenized Ecosystem of Personal Data—Exemplified on the Context of the Smart City	2017	2
					ACM Web Science	In Workshop on Economics and Surveillance		Privacy by Obfuscation with Personal Data Management Architectures: Possibilities and Constraints	2015	3
					Edições Sesc			Everything about Every@ ne: Digital Networks, Privacy and the Personal Data Trade	2017	2
					Richmond		Journal of Law and Technology	Artificial Intelligence and Governing the Life Cycle of Personal Data	2017	1
					diva-portal.org			Mergers in big data-driven markets: is the dimension of privacy and protection of personal data something to consider in the merger review?	2018	2
					pacific.edu HeinOnline		Global Business & Development Law Journal	Protecting Consumer Data While Allowing the Web to Develop Self-Sustaining Architecture: Is a Trans-Atlantic Browser-Based Opt-In for Behavioral Tracking the Right Solution?	2013	11
							Journal of Information Policy	Defining the Limits of Governmental Access to Personal Data Stored in the Cloud: An Analysis and Critique of Microsoft Ireland	2017	2
					cresse.info			User Data and Platform Competition	2017	2
				C	sagepub.com		International Journal of Distributed Sensor Networks	A distributed collaborative platform for personal health profiles in patient-driven health social network	2015	8
				Regional		El profesional de la información (EPI)		Privacy concerns about information sharing as trade-off for personalized news	2018	3

Appendix F: Online Survey



A Study on Personal Data Monetisation in UAE

Thank you for your interest in participating in this research.
Before you agree to take part of this questionnaire, please read the information below which explains the research.

The research aim is to conduct a study on the knowledge and awareness of monetising user's personal data in order to get a return benefits value as service, money, etc.
This research is a meta-analysis on this topic and it will be focused on UAE.

If you have any questions or concerns regarding the research, please contact Reem Al Falasi on the following email address 20170324@student.buid.ac.ae, otherwise continue on to give your consent and take part in the questionnaire.

*Required

I confirm that: *

- [ ] I have read the information provided above and understand the purpose of the research.
- [ ] I understand that I can stop answering questions at any time by navigating away from the survey pages.
- [ ] I consent to the storing and processing of my data for the purposes of this research. I understand that such information will be treated as strictly confidential.
- [ ] I understand that any free text or comments I enter may be quoted, anonymously, in resulting reports.
- [ ] I know who to contact if I have any questions or concerns about the project.
- [ ] I agree to take part in this research.

NEXT

Page 1 of 3

Demographics Data

What is your gender? *

- ◯ Male
- ◯ Female

Which category below includes your age? *

- ◯ Under 18 years
- ◯ From 18 to 24 years
- ◯ From 25 to 34 years
- ◯ From 35 to 44 years
- ◯ From 45 to 54 years
- ◯ Above 55 years

What is the highest degree or level of school you have completed? If currently enrolled, select the highest degree received. *

- ◯ High School
- ◯ High school graduate, diploma or the equivalent
- ◯ Bachelor's degree
- ◯ Master's degree
- ◯ Doctorate degree
- ◯ Other: _____

Which of the following categories best describes your employment status? *

- ◯ A Student
- ◯ An employee
- ◯ A self-employed
- ◯ A housewife
- ◯ Unemployed
- ◯ Unable to work
- ◯ Other: _____

What is your nationality? *

Your answer

Place of residence *

- ◯ Inside UAE
- ◯ Outside UAE

*Required

The research questionnaire

Have you ever shared your personal data/information with anyone? *

- ◯ Yes
- ◯ No
- ◯ Maybe
- ◯ Other: _____

If yes, would you please mention what kind of your personal data/information that you had shared?

Your answer

Will you agree to share your personal data/information with a trusted company that you are confidante of their personal data privacy policy? *

- ◯ Yes
- ◯ No
- ◯ Maybe
- ◯ Other: _____

What are the main factors/things that you make sure of before sharing your personal data/information? *

Your answer

Will you agree to share your personal data/information in order to get a new service? *

- ◯ Yes
- ◯ No
- ◯ Maybe
- ◯ Other: _____

Will you agree to share your personal data/information in order to get new a personalised service ? *

- ◯ Yes
- ◯ No
- ◯ Maybe
- ◯ Other: _____

Will you agree to share your personal data/information in order to get an offer on your interested service? *

- ◯ Yes
- ◯ No
- ◯ Maybe
- ◯ Other: _____

If yes, please identify what is the interesting service, that you will agree to share your personal data/information to get an offer in.

Your answer

Will you allow any company to share your personal data/information with other company in order to provide to you the best service/offer ? *

- ◯ Yes
- ◯ No
- ◯ Maybe
- ◯ Other: _____

Will you allow any company to share your personal data/information with other company without paying you or providing any service/offer to you? *

- ◯ Yes
- ◯ No
- ◯ Maybe
- ◯ Other: _____

Will you agree to get paid in order to share your personal data/information? *

- ◯ Yes
- ◯ No
- ◯ Maybe
- ◯ Other: _____

Do you prefer to get money from sharing your personal data/information rather than work or look for a job? *

- ◯ Yes
- ◯ No
- ◯ Maybe
- ◯ Other: _____

Will you agree to share your personal data/information, if you have the control to choose the exact personal data, that you would like to share it with someone trustworthy? *

- ○ Yes
- ○ No
- ○ Maybe
- ○ Other: _____

Do you agree to share your personal data/information with an insurance company to protect your personal data? *

- ○ Yes
- ○ No
- ○ Maybe
- ○ Other: _____

What are your main concerns/worries about sharing your personal data/information? *

Your answer

Please share your feedback and suggestions to improve this research.

Your answer

BACK SUBMIT Page 3 of 3