The Global Effects of the General Data Protection Regulation

Foreign Business, Competition, and Innovation

Student Name: Inna Storchak
Student Number: 491544

Supervisor: Payal Arora

Master Media Studies - Media & Business
Erasmus School of History, Culture and Communication
Erasmus University Rotterdam

Master Thesis
June 7th 2019

The Global Effects of the General Data Protection Regulation

Abstract

As a result of rapid advancements in digital technologies over the course of the last decade, European data security and privacy laws became rapidly outdated and ineffective. Following a number of high profile security incidents and privacy scandals, the European-wide General Data Protection Regulation (GDPR) came into effect in May of 2018. The regulation, however, does not only apply to businesses within the EU, but also to any company which controls or processes any data pertaining to European citizens. This global scope consequently raises a number of concerns regarding the global effects these new laws may have, their applicability outside the West, and whether the laws will set a new golden standard for data and security practices. With a focus on business, this thesis uses qualitative methods, particularly Critical Discourse Analysis in order to examine the extent to which the GDPR may create a fairer and more inclusive regulatory framework in the global digital economy. A variety of diverse reports, blogs, and academic papers concerning data, privacy, innovation and other relevant elements were sampled in order to understand the current conflicts and debates within the data sphere, as well as unpack the cultural assumptions that behind the GDPR. Results indicate that a global improvement of privacy standards and data practices is becoming increasingly evident and urgent. However, while the necessity for GDPR, and similar regulation is understood, there are a number of concerns still hindering its effectiveness, such as digital inequalities, cultural differences, as well as corporate and political influence. Further, according to the media, while enterprises of all sizes which fall under the scope of the GDPR will be affected, the most impact will fall on tech giants and large corporations. However, the debate as to whether this impact will be beneficial or detrimental is still ongoing. Finally, the findings indicate a number of long term, global effects triggered by the regulation and the resulting discourse, such as changing attitudes towards privacy and transparency.

KEYWORDS: *GDPR, Privacy, Data Protection, Competition, Global*

Table of Contents

Chapter 1: Introduction

Over the years, since the early days of data sharing, digital privacy has been growing into a significant area of public and academic interest. With the recent, high profile privacy breaches and scandals, data protection is more important than ever when it concerns both organizations and individuals. The Ashley Madison hack, Equifax data breach, and the Cambridge Analytica-Facebook scandal are only a few examples of these issue. The consequences of these data breaches can be immense, from the misappropriation of personal data for advertising purposes, to using the information to influence political elections. In the decade leading up to the introduction of the General Data Protection Regulation (GDPR), while being more necessary than ever, European privacy laws were outdated and could no longer meet the difficulties of globalization and technological development. The European-wide digital privacy regulation came into effect in May 2018, succeeding the outdated Data Protection Directive (DPD) which was adopted to regulate private data in 1995 (Rubinstein, 2013). Following its implementation, a number of debates about privacy and innovation, as well as what constitutes appropriate data practices if GDPR globalizes arose.

A number of significant changes emerged with the updated laws that reflect technological evolution, most notably related to the way businesses collect and handle personal data. In an age where "big data is the new oil," these changes are especially meaningful (Mayer-Schönberger & Cukier, 2013; McAfee & Brynjolfsson, 2012). Primarily, a more expansive definition of what constitutes as 'personal data' has been established to include information such as IP addresses, geolocation, and biometric data. In addition to this, any other information that can lead back to an individual, such as mental, genetic, economic and social identity are now also included in this definition (SeeUnity, 2018). Another significant change, is that the law allows individuals within the EU to have greater control over what type of data is collected, who may collected it, as well as how this data is being used. User agreements are now required to be transparent – understandable and to the point – and separate consent for different types of data is explicitly required. In addition to this, under the "right to be forgotten" clause of the regulation, a user may not only view all the information gathered about them, but also delete it entirely (Politou, Michota, Alepis, Pocs, & Patsakis, 2018). Further, under the GDPR, both the controllers – those who collect and store the data –, and the processors – those who use it – will be liable and responsible for securing it. This means that a third party that collects and analyses data by another organization's behalf will also be held accountable for any violations (Beaumont, 2018). Companies and organizations that do not comply with the law will face harsh consequences, for example, having their online traffic blocked, and fines of up to 20 million euro, or 4% of their total revenue (European Commission, 2018a).

This study will focus on the under-researched global implications of these European regulations. While the GDPR has provided a comprehensive blanket regulation which is uniformly applicable throughout all EU countries, these same laws also encompass foreign businesses that operate in European markets. Under the new regulations any business, even if located outside Europe, will have to adhere to the same laws as long as it offers services, processes or holds any data pertaining to an EU subject (European Commission, 2018a) . This global application of regulation has sparked debate amongst scholars. A number of studies hypothesized that due to the international reach of the GDPR, a new gold standard for the way private information is handled around the world will be set, while simultaneously improving encryption and security measures worldwide (Mansfield-Devine, 2016; Safari, 2017). Additionally, through applying equal laws to all, the GDPR could potentially create a positive, more individual and consumer-centric system for innovation (Albrecht, 2016; Ciriani, 2015).

In contrast, the other side of this debate argues that the regulations will create a barrier for smaller businesses, hinder innovation and encourage monopolization (Bartlett & Ghoshal, 2000; Couldry & Mejias, 2018). Primarily, while large corporations possess sufficient resources to manage the new regulations, the GDPR could place too much of a financial burden on smaller companies, which would deter their competition within international markets (Gallagher, 2018; Wilkinson, 2018). Couldry and Mejias argue towards this point in their study which discusses the idea of 'data colonialism,' created through an uneven distribution of data power (2018). Inhibiting the competition of smaller companies by financial constraints, GDPR would aggravate the data monopolization that we can observe amongst tech giants such as Amazon, Google and Facebook (Andrejevic , 2014). Smaller companies' inability to compete will consequently hinder technological innovation in the tech markets. These tensions between privacy laws and innovation have been the subject of a number of studies (Goldfarb & Tucker, 2012; Santanen, 2019; Zarsky, T. 2017). The general consensus is that while an appropriate governmental response to data collection practices is needed, there is an undeniable relationship between such regulations and innovation.

The final dimension of the privacy debate addressed in this thesis, are the cultural assumptions that are often made when discussing privacy issues (Arora, 2018). Nations across the world share different, and often conflicting cultural values and ideals. The manner in which privacy is perceived, and the importance placed on it also differ. The GDPR is mainly Eurocentric and was created from a Western perspective. Therefore, one can argue that while the regulations are a step in the right direction, they are not sufficiently inclusive to qualify as a new global standard for digital privacy.

Considering the debates and findings of currently existing literature, the thesis will use critical discourse analysis in order to examine and answer the following research and sub- questions:

RQ: To what extent is the General Data Protection Regulation creating a fairer and more inclusive regulatory framework in the global digital economy?

Sub-question 1: In what way could the General Data Protection Regulation affect technology enterprises outside the EU in terms of competition and innovation?
Sub-question 2: What are the underlying assumptions behind GDPR and how may they be culturally-biased?

Following this introduction, chapter 2 of this paper examines and evaluates the existing literature regarding privacy practise, data, innovation, as well as the impact of these elements on various enterprises. The theoretical framework which this research will be based on is also outlined. The 3rd chapter provides a detailed description of the methodology used, explains the reasoning behind the sampling, and considers a number of possible limitations. Chapter 4 presents and interprets the findings results, as well as considering them in relation the theories discussed in chapter 2. Finally, chapter 5 concludes the study through a discussion of the findings, answering the research question, as well as making a few suggestions for future research.

Chapter 2: Theoretical Framework

The following chapter will outline and review the theories and existing literature related to the research question. Concepts are defined and explained in context of privacy and the GDPR. Primarily, Data protection, and the idea of privacy and how it varies culturally and across nations is discussed. The second section examines the tensions between privacy and innovation, followed by a discussion related to the regulations' transfer of power to the individuals in the third section. Finally, the last section covers concerns related to big data.

2.1 Understanding Privacy and Data Protection

Privacy is a significant, highly discussed, but constantly evolving issue in the modern age, and it is important to properly define and understand this concept in the current, digital context. Throughout the years, scholars have proposed a variety of definitions based on diverse disciplines (Dinev et al., 2012, Moore, 2008). A number of documents describe privacy as control over personal information and what one chooses to communicate to others (Solove, 2008; Westin, 1967). Louis Henkin (1974) and others similarly maintain that privacy is ones independence, "to be free from unwanted intrusion," (p.1419) to be free from publicity, and the right to keep private information undisclosed. Roger Clark has proposed that rather than privacy being a single entity, it consists of multiple dimensions (2006). These dimensions include "privacy of the person," which involves an individual's physical attributes such as blood, organs and bodily procedures such as sterilization and abortion; "privacy of personal behavior," such as habits, religious beliefs and sexual preferences; communication privacy, which refers to undisclosed communication without unwanted monitoring; and finally, data privacy. Data privacy, often also referred to as information privacy, is an individual's ability to control the spread personal information about oneself online. With further evolution of the internet, and the exponential growth of technology and available information, our understanding of privacy has been shifting and becoming increasingly difficult to define (Solove, 2008). To accommodate for the technological progress, others have been expanding Clark's dimensions of privacy (Finn, Wright & Friedewald, 2013). Ultimately, based on the basic description as "the right to be left alone," our understanding of privacy has broadened from the privacy of the self, to include data and the digital world, and has become equally comprised of personal, information, as well as communication components (Hung & Wong, 2009; Warren & Brandeis, 1890). With identities becoming increasingly reflected in the digital world, data protection has transformed to be a significant dimension of personal privacy, with privacy conversations now being filtered through the data lens. Privacy is not just about the self, but also individuals' online selves, which are constructed through personal data in a variety of diverse forms. Under the GDPR, this discourse, as well as data variation, is demonstrated in its expanded definition of personal data.

2.1.1 Datafication and Privacy Across Cultures

One of reasons why defining and understanding what qualifies as private is difficult, is due to differences in cultures and social norms. In the Western world, the notion of privacy is maintained as an extremely significant, valuable element of society, an intrinsic principle necessary for preserving our "integrity as persons" (Fried, 1968). As discussed in his thesis, Charles Fried states that in the West privacy is perceived as an integral element for the construction of respect, love, friendship, and trust (1968). Reiman similarly explains how all other fundamental rights are derivative from the right to privacy, and without it "intimacy and personhood" are lost (1976). However, the understanding of, and importance placed on privacy varies even across the Western world (Whitman, 2004). For instance when considering Europe, a union that ostensibly shares similar beliefs and attitudes, there is an evident divide in approaches towards data management and disclosure, which affects privacy concerns (Miltgen & Peyrat-Guillard, 2014). These differences of perception are even more pronounced outside of the West. While the Western world places great moral and legal importance on privacy, this is not necessarily the case elsewhere. Examining these views of privacy in context of the GDPR and global standards is significant as these may reveal such culturally biased assumptions, and consequent effects on enterprises outside the EU.

A number of studies have demonstrated a relationship between culture and privacy perception, concern and desire for awareness. Hofstede's cultural dimensions were shown to often be a significant indicator of the effects one's nationality, and cultural background may have on privacy perception (Lowry, Cao & Everard, 2011; Cho, Rivera-Sánchez & Lim, 2009; Cao & Everard, 2008). According to Hofstede, cultures center around six main dimensions – power distance, individualism vs. collectivism, uncertainty avoidance, masculinity vs femininity, long-term vs. short term orientation and indulgence vs. restraint (Hofstede & Triandis, 1993). These dimensions are often used to interpret behavior within various cultures or nations, and were shown to be significant predictors of privacy concerns (Lowry, Cao & Everard, 2011). For example, apparent differences in privacy attitudes between those from individualistic societies, such as Australia and the United States, and collective societies, such as Singapore and Indonesia can be seen (Cho, Rivera-Sánchez & Lim, 2009). Individualistic cultures exhibited more concern, and were shown to perceive privacy as more important in contrast to collectivistic cultures, who more easily accepted intrusions into individual privacy (Liu, Marchewka & Ku, 2004; Milberg, Burke, Smith & Kallman, 1995). However, Hofstede's theory of cultural dimensions is widely used and considered a classic in culture studies, it has also been criticized for determinism and culture flattening – the oversimplification of national values and idea that human beliefs and behavior are caused by external factors (McSweeney, 2002).

Moreover, despite the world becoming more connected, and cultural differences made increasingly salient, privacy studies and most existing literature, still mostly examine this concept from the Western perspective (Arora, 2018). Based on a multitude of similar cultural assumptions, the GDPR is one such regulation. Privacy is considered through a Eurocentric framework and Western perspective. These types of regulations do not necessarily consider cultural differences, and are consequently not fully inclusive. Despite these shortcomings, the GDPR is globally enforced with nations outside the EU being affected, and is said to be a new golden standard for privacy and security.

Moreover, it is also important to consider the current data architecture, which allows for the violation and exploitation of privacy through the immense quantities of data which we are generating globally. According to Cisco's whitepaper report, global IP (Internet Protocol), inter-device traffic should reach 201 exabyte (EB) this year, and predicted to keep rising to 396EB by the end of 2022 (Cisco Systems, 2019). To put these numbers into perspective, if a 2 hour, high quality movie requires approximately 5 gigabyte, then an EB can store 5 billion movies (Williams, n.d.). As demonstrated by the report, the data growth is not likely to diminish. In reality, the amount of varied forms our information may be expanding. Some examples of the more evident information systems that generate data include visual content, such as images and video, written content, like articles, emails or comments on social media platforms and forums, and financial information that may be related to retail, pay checks or stock exchange records (DOMO, 2018). With this growth of data generation, and the existence of social networks and apps, the 'sharing' of private information has gradually become normalized (Van Dijck, 2014). Further, the Internet of Things (IoT), and developments such as the emerging 5G network also contribute to data creation. IoT is the addition of a digital component – internet connectivity - to everyday objects, such as watches, speakers or even air conditioning units (Atzori, Iera, Morabito, & Nitti, 2012). As the internet increasingly becomes an essential component of everyday life as a result of this connectivity of common household objects, privacy and security concerns increase as well. Such devices are able to digitally document everyday activity, such as individual movement and location, personal interests, habits, communication, and so on (French & Shim, 2016). This coding and translation of human behaviour into digital information is referred to as datafication, the process that allows for surveillance and predictive analysis (Van Dijck, 2014). While some of this information, for example simple 'Facebook Likes,' might appear innocuous in context of privacy or security (particularly when compared to other forms such as location data), this is an erroneous perception. As demonstrated by Kosinski and his peers, this seemingly inconsequential information can, in reality, be used to accurately deduce highly personal information such as sexual orientation, age, ethnicity, religious affiliation and

a range of specific characteristics (Kosinski, Stillwell & Graepel, 2013). In consideration of this climate where privacy can be easily violated through such diverse forms of data, and the amount of personal information can be extracted, the need for security and its protection becomes increasingly urgent.

2.1.2 Small and Medium Sized Enterprises and Data Regulation

In order for a business to survive and effectively compete in the modern age of globalization, being active in international markets is vital (Taylor & Fosler, 1994). This not only includes large international corporations, but also personal brands, and smaller enterprises (Bell & Loane, 2010; Taylor & Fosler, 1994). Increasingly, these small businesses are breaking into the global markets and catering to international consumers (USForex, 2016; Taylor & Fosler, 1994). With the majority of European businesses being composed of small or medium sized enterprises (SMEs), predictions on how the GDPR would affect them once it came into effect were widely conflicting (Wilkinson, 2018). One perspective is that due to the scope and effect of regulation, the law would place too much of a financial burden on smaller companies, which would discourage growth, competition, and consequently innovation (Wilkinson, 2018). SME's lack the resources of larger corporations, yet are under the same pressure to cover all aspects of their activity (Gallagher, 2018). As argued by various studies, privacy regulations such as the GDPR could either facilitate, or interfere with innovation (Zarsky, 2017). The role of laws and regulation in technological development and innovation is discussed by Chander in his study, where the author compares practices throughout the US, Europe and Asia (2013). According to this study, the reformed copyright and tort laws (which reduced the risks of traders), and lack of strict privacy regulation allowed for the rapid and successful development of Silicon Valley, as well as other technological hubs in the US. Those in Europe or Asia, specifically Japan and South Korea, developed considerably slower as a result of legal obstacles as "the laws of these regions are far less conducive to Internet enterprise than the United States" (Chander, 2013, p.670). However, while this is an interesting theory, the study is based on expert opinion and correlation, and as of yet there is no direct empirical evidence that the EU has not produced their own silicon valley solely as a result of privacy regulation. Furthermore, overall Asia has been known to either lack, or have comparatively relaxed, and lenient privacy regulations (Privacy International, 2013). The privacy concern of a nation has also been linked to the level of regulation and government involvement (Bellman, Johnson, Kobrin, & Lohse, 2004).

In contrast, others have argued that the strict requirements of the regulation may be globally beneficial in the long run, and will provide a new, global security standard. In his study, Mansfield-Devine discovered that forcing smaller companies in particular to tighten their security standards is extremely important. Due to their size most do not consider themselves to be significant

enough to target, and consequently do not take sufficient measures to protect themselves from breaches. In reality, these SME's can be used by malicious agents as a stepping stone into the networks of bigger corporations (Mansfield-Devine, 2016). Through creating a consistent, multinational regulation concerning data rights and protection, the GDPR forces improved security standards on companies and organizations, while simultaneously allowing European citizens better control over the information that is processed and collected (Beckett, 2017).

2.2 Privacy and Innovation

In order to answer the research question, a significant element to consider within privacy discourse is its relationship with innovation, as well as effects on competition. The GDPR's global scope, and heightened requirements add a new and critical variable to the digital economy, which could result in the disruption of the flow of information, thereby affecting the enterprises reliant on vast amounts of data. Furthermore, the conflicts within said discourse may reveal the stakeholders and power dynamics interests within the data sphere.

2.2.1 Digital Innovation and Big Data

'Big Data' is another significant concept which according to a number of scholars could be affected by the privacy regulations. Historically, with the development of computer technologies, the term data constituted any information regarding computing (Puschmann & Burgess, 2014). Gradually, as technology proliferated and evolved, the variety and quantity of data also increased. Thus, the term 'big data' emerged from within the business world, referring to large, complex volumes of digital information, which may be collected, analyzed, and interpreted to uncover patterns (Puschmann & Burgess, 2014). Big data analysis has provided an array of innovative solutions to issues across various business sectors, such as finance, healthcare, and retail. While some scholars criticize the potential negative effects of such data analysis, such as negative effects on privacy and intrusive marketing tactics, others have cited a multitude of benefits (Boyd & Crawford, 2012). Making data-driven decisions, and effectively using data-derived information can advance a business, as well as allow for a better understanding of one's market and consumer needs (LaValle, Lesser, Shockley, Hopkins & Kruschwitz, 2011; Crié & Michaeux, 2006). Often referred to as 'the new oil', data analysis is considered to be a highly valuable commodity, and carries the aspiration to provide improved solutions to a magnitude of societal issues (Xiaolong,Wah, Cheng & Wang, 2015).

The GDPR, however, may pose a number of issues and barriers to data analysis and thus the advantages it can provide for business and innovation. Big data analysis is a significant aspect to an

array of both large and small businesses in their daily function. Privacy laws and regulations on the other hand are said to be inherently incompatible with big data, and would make its analysis "suboptimal and inefficient"(Zarsky, p. 996, 2017). In his study, Zarsky outlines a number of points within the GDPR which disadvantage big data (2017). For example, since technically only the collection *necessary* data is permitted under the regulation, data controllers would become more stringent with what data is used, and, as the information is only to be gathered for a limited, specific purpose said data would be limited. Big data analysis on the other hand relies on more complete information in order to be optimal. This is its reliance on quantity – the more data, and the more complete the information, the more effective big data analysis will be. Things such as pattern recognition and prediction algorithms are based on extensive social information, as opposed to individual actions. Another significant obstacle, although the least likely to be enforceable aspect of the GDPR, is article 22, which allows individuals to choose to be entirely excluded from any automated processes (Zarsky, 2017). Cunningham similarly referred to the right to be forgotten as 'disguised censorship,' (2016, p. 95), pointing out that currently there is no governmental supervision which evaluates and determines the type of data that is to be removed. Additionally, no criteria exist on what justifies the deletion of certain data, apart from it being considered personal. According to the scholar, this type of manipulation would create content inconsistencies, knowledge gaps and "disrupt[s] the natural process of communication" (Cunningham, 2016, p. 96). Further, while comparable clauses were also present in the DPD, they have a much greater impact under the GDPR due to its global reach, and will therefore affect more organizations in their daily operations.

2.2.1.1 Data Sovereignty

The International Data Corporation (IDC) have predicted that this year, in 2019, the global spending in regards to the internet of things may rise to $745 billion, and exceed $1 trillion around 2022 (IDC, 2019). This is one significant indicator of the value of big data. Consequently, the enterprises that are able to collect and utilize this data will possess more power and opportunities within the digital market. While the majority of data is currently managed by private parties, governments began recognizing its value, and are increasingly taking an interest and participating (Alemanno, 2018). The implementation of the GDPR, as it is based upon the collection of data, is an indication of this governmental interest. This holds a number of implications for the free market and sovereignty of data. Data sovereignty refers to the information being under the jurisdiction of the laws in the nation where it is stored, contradictory to the borderless nature of the online world (R&G Technologies, n.d.). This concept, in conjunction with regulations that heavily affect data, allows for increased governmental control over the information, while simultaneously obstructing the free markets. Such constrictions on the previously borderless flows of data, as well as conflicting

interests in information control may also affect tech enterprises in terms of competition and innovation.

2.2.2 The privacy-innovation conflict

The relationship between privacy laws and innovation are often a point of concern in literature and policy making which has been examined in numerous studies. Modern technology allows companies to collect and utilize vast amounts of personal information, which may provide an avenue for improvement in their daily function. However, the trade-off for such data-driven innovation comes at a cost of personal privacy, as potentially intrusive information is gathered, often without the knowledge or proper consent of the user. Consequently, the introduction of the GDPR raised a number of questions regarding how the strict privacy laws may affect innovation. While some argue that a global, blanket regulation will equalize opportunity for all enterprises, others insist that the innovation and competition of smaller enterprises (SMEs) may be hindered.

Using data can generate knowledge, advance analysis technologies, as well as enhance business models by observing customer behavior (Zarsky, 2015). Enterprises can also better understand their target market, as well as refine the product and services based on the collected data (Goldfarb & Tucker, 2012). While these processes contribute towards innovation, privacy regulations are said to impede this development through diminishing the flow of data. Additionally, compliance to GDPR regulations creates additional financial burdens; this causes interruptions in business processes and results in uncertainty which may further deter innovation (Zarsky, 2015). As a result of such compliance issues, the GDPR may not only hinder innovation, but create a barrier for smaller businesses, as well as encourage monopolization (Bartlett & Ghoshal, 2000; Gallagher, 2018; Couldry & Mejias, 2018; Wilkinson, 2018).

On the other hand, through applying equal laws to all, the GDPR could potentially create a positive, more individual and consumer-centric system for innovation (Albrecht, 2016; Ciriani, 2015). Zarsky further argues that while there are disadvantages to strict privacy laws, they can also in certain instances lead to social and market innovation by increasing trust and creativity (2015). The scholar states that when individuals understand and trust that their private information will not be misused, they will feel more secure and likely to engage with online services. Provided that the business is motivated and willing to independently set the privacy safeguards that will generate consumer trust, the consequent engagement may promote innovation. As individuals are becoming increasingly aware of the information tracked and collected about them, the demand for transparency in how this information is used, particularly private information rises (Phelps, Nowaak & Ferrell, 2000). Improved security and privacy standards such as those imposed by the GDPR may thereby increase trust and provide a competitive advantage for SMEs.

Alternatively, while discussing the relationship between surveillance and privacy, Julie Cohen states in her that the idea of innovation being an 'autonomous,' 'freely flowing,' and 'inevitably beneficial' mechanism is a rhetoric fabricated by agents who may benefit from unrestricted flows of information (Cohen, 2019). Regulators on the other hand disagreed with the idea of innovation being more important than privacy in the digital age, instead accepting the "relationship as one of conflict"(Cohen, 2019, p.8). Therefore, the privacy-innovation conflict can be more accurately interpreted as a tension between certain power interests involved in the data discourse – those who benefit from unrestricted data flows, and those who in favor of more substantial privacy and security standards. Therefore, while some stakeholders claim that a lack of privacy and excessive surveillance may encourage innovation, this might be a somewhat bias view and not necessarily the case.

2.2.3 Responsible innovation

Further, in recent years considerable emphasis has been placed on the fact that innovation should prioritize social wellbeing and be held accountable to the public. This is reflected in the GDPR as despite it being a potential barrier to innovation in general, it can also be viewed as the aperture that encourages responsibility. While the outdated European laws could no longer meet the difficulties of globalization and responsible technological development, the GDPR demands a balance between privacy and innovation.

Responsible innovation, a concept that has been emerging throughout literature in the last decade, refers to scientific research and technological development that considers the impact on environmental and social well-being (Blok & Lemmens, 2015; Stilgoe, Owen, Macnagehten, 2013; Von Schomberg, 2013). Historically scientific exploration has been unrestrained by policy, allowing for the innovation of various technologies without political interference (Stilgoe et al., 2013). While beneficial to scientific autonomy and generating knowledge, this conflicted with the more ethical responsibilities to society (Douglas, 2003). However, as the potential negative impact of ungoverned innovation became more evident, a shift to holding research to higher ethical standards occurred (Blok & Lemmens, 2015; Groves,2006). In the business context where society is considered a significant stakeholder, responsible innovation aims to balance economic, environmental and social elements (Block & Lemmens, 2015). Privacy, when considered as a valuable social interest falls in the realm of responsible innovation. As discussed, the intertwining and integration of technologies into everyday life consequently provides the ability for businesses to use and collect data, consequently exacerbating privacy concerns. This is therefore a salient element of social life that responsible innovation should acknowledge (Stahl, 2013). The implementation of the GDPR reflects the importance placed on privacy by European society, emphasizing the need for responsible

innovation which specifically takes this element into account. The regulation can be seen as an attempt to not only rectify concerns related to privacy, but also promote responsibility by striving for a balance between privacy and innovation.

2.2.4 The Big Data Divide

Proposed by Andrejevic in his paper, the big data divide is a concept referring to the disproportional relationship amongst data controllers - those who collect, store and utilize big data - and those who create and are targeted by the data (2014). While the ability to access and somewhat control private information implemented the GDPR may potentially bring more balance between the two sides of the divide, users would still be unable to take advantage of big data the same way corporations can. This is because as mentioned previously, big data relies on quantity, while the data generated by a single person would not produce the same results. Additionally, individuals do not have access or the sufficient capability and resources for such analysis. So, while regulations provide greater individual control over data, they may not full balance the sides that are able to take advantage of it, but rather digitally mirror the imbalances of the real world.

> The sense of powerlessness that individuals express about emerging forms of data collection and data mining reflects both the relations of ownership and control that shape access to communication and information resources, and growing awareness of just how little people know about the ways in which their data might be turned back upon them. (Andrejevic, 2014, p.1675)

This imbalance contributes to individual lack of agency, as well as reinforcing the market dominance of the select number of organizations – tech giants such as Google and Facebook. This division that has been noted by Boyd and Crawford (2012) - the divide between “the Big Data rich” – companies and large elite universities that have the means to generate or procure, as well as store vast amounts of data – and “the Big Data poor”- those excluded from access to such data, without sufficient expertise or processing power (Boyd & Crawford, 2012).

2.2.5 Transfer of Power to the Individuals

As previously stated, the GDPR has introduced a number of notable changes to European privacy regulations that allow the creators greater individual control. Primarily, a more expansive definition of what constitutes as ‘personal data’ has been established to include data such as IP addresses, geolocation, and biometric data. Any other information that can lead back to an individual, such as mental, genetic, economic and social identity are now also included in the definition (SeeUnity, 2018). Control over the collection and usage of one’s personal information, and mandatory user-

agreement transparency established by the regulations may potentially transfer agency into the hands of everyday citizens (Alberecht, 2016). While this seems like a step in the right direction regarding the data divide, online security and information control, a number of concerns and challenges emerge once these features are applied to a global context. As well as the Euro- centric cultural expectations, the regulation is based on the assumption that there is a homogenous level of digital and privacy literacy. In reality, the digital divide, as well as varying levels of digital literacy may pose a number of issues with this transfer of power to the individuals. Nevertheless, whether this provision of increase of control over private data is effective or not, it is useful to examine how this shift within the power dynamic may affect various enterprises.

2.3 Digital Literacy

Before the digital era the term 'digital divide' illustrated the separation of those with physical access to a telephone or a computer, and those without. As technology developed, the measure of available information rapidly grew, and our dependence on the online world increased, the divide now referred to the inequality in access and ability to use information technologies (Van Deursen & Van Dijk, 2011). According to Van Deursen and Van Dijk, since technology has proliferated in the modern world, the divide further narrowed to simply represent the disparity between the skilled and unskilled. This level of skill can also be understood as digital literacy – the ability and expertise in effectively accessing information – is a significant advantage in the modern world (Digital Literacy, 2018). The global digital divide refers to the variation of access, usage, and degree of literacy amongst cultures, countries or regions. Economically disadvantage nations, even those that do have large numbers of smartphones, often lack sufficient digital literacy. Socio-economic status, education structures and certain cultural factors were further shown to influence digital proficiency (Robinson et al., 2015). Those with higher education and digital literacy skills were shown to engage in more "capital enhancing" activities online, further demonstrating differences in digital skills among the populations (Hargittai & Hinnant, 2008). While the GDPR is a step towards a more user-centric internet, in practice these differences in literacy may be a barrier to the regulation of setting a new universal, golden standard for security and privacy control. As internet skills are not homogenous, the transfer of agency and ability to control one's own privacy to citizens may not be entirely effective.

On the other hand, it can also be argued that the ability to access and navigate information does not necessarily guarantee that individuals are educated enough to be able to make the 'right' choices. As pointed out by Boyd, there is an overabundance of information in the digital age, not all of which is accurate or truthful (2017). As a result, communities have diverse, culturally influenced approaches for discerning what is considered trustworthy; individuals are taught to question

information, as well as the authority of media sources, and work out for themselves what is true. This is further exasperated by the fears of the spread of misinformation such as 'fake news,' which is rapidly becoming a global issue, and propaganda, such as the one taking during the recent US election (Connolly et al., 2016). Further, even if an individual is presented with accurate, and truthful information, it might not be accepted. This is a common psychological phenomena known 'The Backfire Effect,' – a form of confirmation bias - where individuals are likely to resist information that contradicts their beliefs, and as a result the information solidifies their original stance (Silverman, 2011). Therefore, even if digital literacy is globally homogenous as the GDPR assumes, transferring the power, and responsibility to control their own data onto individuals may not lead to a favorable improvement.

Furthermore, the privacy paradox is another factor which poses an issue in applying regulations as extensive as the GDPR. This paradox refers to the dissonance of perceiving ones' private data as extremely significant, but also being willing to sacrifice this privacy for a relatively small reward (Wong, 2017). This contradiction of one's belief that privacy is valuable, and the behavior of easily giving it up is a reoccurring phenomenon throughout literature regarding digital privacy and security (Kokolaki, 2017; Norberg & Horne, 2007). When it comes to agreements in sharing persona information, warnings and notices are very often ignored by the users (Kuner, Cate, Millard & Svantesson, 2012). Even in cases where attention is brought to the notices, such as those related to tracking cookies, or the currently commonplace GDPR notices, users are more likely to make the choice which will allow them access to a website or service. Thus, despite the regulation establishing mandatory transparency in user agreements and individuals being able to understand these more easily, privacy may still be willingly sacrificed to corporations in favor of accessing a desired product, or a more personally-tailored online experience.

2.3.1 The Right to be Forgotten

Another regulatory addition that has to be addressed is the "right to be forgotten" clause which allows the users to not only view all the information gathered about them, but also delete it entirely (Politou, Michota, Alepis, Pocs, & Patsakis, 2018). An earlier iteration of this amendment did exist under the DPD, however the controllers – those who collected, stored and used the data – were solely responsible for safeguarding the data which was considered personal or sensitive. This placed responsibility on corporations such as Google or Yahoo. The introduction of this element sparked global debate in regards to whom should be accountable for protecting personal data, and as argued by Abril and Lipton (2014), it was "unbefitting and socially undesirable" (p. 363) for businesses to bear this responsibility. Further, this was extremely difficult to enforce, and very little governmental oversight existed. Now, with the GDPR succeeding the outdated DPD, this

responsibility has shifted from solely corporations to also include individuals. The 'right to be forgotten' was created as a response to the threats on personal privacy posed by the internet, yet a number of issues arise when applying it to a global context. The most significant of these difficulties, are the contradictions between this right and existing laws in other cultures, and potential dangers of censorship in non-democratic nations.

When the amendment was first introduced during the days of the DPD, various scholars identified a number of issues in context of the US's freedom of speed and expression laws (Fazlioglu, 2013; Larson, 2013; Bennett, 2012; Weber, 2011). It was argued that the element may promote, and justify censorship, making if incompatible with American culture. When facing large fines, it may be anticipated that corporations would choose to err on the side of caution choose to remove information rather than conserving it in the name of free speech or artistic expression. Further, the right to be forgotten has so far not been explicitly defined, therefore leaving the issue, and what falls under the category of artistic expression open to interpretation, thus further damaging freedom of speech (Fazlioglu, 2013). Those who argue in support of the right to be forgotten, on the other hand, addresses current, urgent issue of digital permanence of information. The objective of the right is to allow individuals autonomous growth, unconstructed by past actions or mistakes, particularly if they took place years ago and have no current significance (Mantelero, 2013). Criminal records for example are often digitally, and permanently stored, denying those who have atoned for their crimes the opportunity for a fresh start (Weber, 2011). It is also argued that those who in their youth have posted 'embarrassing' or stigmatizing content on social media and since have grown and regretted it, similarly should have the ability to escape these mistakes (Rosen, 2011). Such information may be both out of date and inaccurate, and the right to be forgotten establishes a degree of security in terms of piracy within one's personal life.

2.3.1.1 Censorship

Similarly, another issue with the right to be forgotten is one related to censorship. It is not yet clear how this specific element of the regulation will be enforced, and now not only corporations, but individuals are able to act on the deletion of information. The regulation, created by policymakers in Europe is effectively able to affect what an internet user on the other side of the planet will see online, which gives the GDPR an immensely wide scope. This has led to some arguing that in essence the right to be forgotten will promote global censorship under the aegis of protecting individual privacy (Cunningham, 2016; Shoor, 2014). Even now, allowing European residents the capability to entirely erase data neglects the sovereignty of other nations, the laws of the US being one example. To this effect, when discussing the first instance when the right to be forgotten passed in a court case, Jeffrey Toobin (2014) warned that the borderless digital world in which information

is available to everyone may fragment into 'national networks.' Largely censored, governments within these networks may dictate the available information.

A comparable occurrence of such interference by state parties has shown to take place on Twitter (Tanash, Chen, Thakur, Wallach & Subramanian, 2015). Governments, and other accredited reporters are able to request the removal of not only data but also entire accounts. In their analysis, Tanash et al. specifically examined Turkey, as it was reported to issue the largest sum of censorship requests (2015). Subsequently, the study uncovered that the number censored tweets was even significantly higher than indicated in the Twitter transparency reports. According to said reports, another nation with high numbers of censorship requests was Russia (Twitter, 2018).

Additionally, a democratic government is another stipulation for the GDPR to function as designed, particularly when it comes to clauses such as 'the Right to be Forgotten', as it could be exploited by perpetrators in authoritarian, non-democratic states. While Russia and Turkey are both democracies on paper, this is not the case in reality (Kerr, 2018). In their report, Dr Lührmann and her team have demonstrated that while global levels are currently shown to remain consistently high, there is an observable deterioration of democratic attributes (Lührmann et al., 2018). 'Autocratization,' was also found to be rising, and affecting as much as a third of the global population, which according to the report indicates a significant decline in the security of rights and freedoms around the world. Undeniably, a correlation between political freedoms, censorship and a nation's type of government can be found; Authoritarian regimes, for instance have been shown to regulating communication technologies, and the spread of information online (Kalathil & Boas, 2001). In such non-democratic states, not only the freedom of expression, but also media autonomy have shown to be deteriorating over the past few years (Lührmann et al., 2018). Moreover, hybrid regimes are also common in the modern age. These are systems of government based on democratic traits such as elections in order to appear legitimate, however are also combined with autocratic characteristics, such as political repression (Gagné, 2015). Consequently, a democracy-based regulation such as GDPR is applied globally, nations under such regimes could potentially exploit certain clauses such as 'the right to be forgotten' in order to further control and censor public discourse.

2.3.2 Developing Nations

As previously stated, while copious studies examine the Western perspective, the attitude, understanding and application of privacy in developing nations, or those in marginalized communities is severely under researched. Despite this lack of research, a substantial amount of speculation arose regarding the possibility of applying the GDPR, or similar regulation to developing nations (Curtiss, 2016). According to Sumner, while global economic growth has raised overall

prosperity, including that of nations of the Global South, no change in economic status has taken place due to inadequate distribution (2016). Approximately 70% of those considered poor are found in developing, middle-income nations not as a result of insufficient resources, but inequality (Sumner, 2016). Meanwhile our understanding of privacy and data practices are similarly Eurocentric. Based on existing literature, the European privacy regulation as well as specific clauses such as the Right to be Forgotten may have a number of effects on data practices in developing nations. Primarily, when considering big data in the context of developing nations, such tech systems tend to be presented as "an instrument of empowerment," and as a result overlooking a number of issues including favoring this type of innovations over privacy concerns (Arora, 2016). Subsequently, data-focused initiatives that encourage the saturation of private information are often supported. As pointed out by Arora, with a lack of sufficient security and privacy regulation, "the big data enables the identification, organization and classification," of marginalized groups and individuals, therefore becoming an instrument of governmental or corporate control (Arora, 2016, p.1689). While governing and regulating big data in developing context may result in a number of advantages, such making welfare systems more accurate and efficient via identification technologies, considerable privacy concerns arise. This same systems, for example, can be used by the governments, or any other agents that collect the information, as a tool for control. Individual privacy, as well as that of high-risk groups and marginalized communities has to be protected.

Regulations such as the GDPR are therefore necessary for preventing harmful data practices as well as providing the citizens with agency and data autonomy. The role of anonymity in developing nations, particularly in non-democratic, authoritarian and oppressive regimes must also not be overlooked, as it is often vital for the well-being of those in marginalized groups (Ganesh, Deutch, Schulte, 2016). In data protection discourse, 'group privacy' is often neglected in favour of individual protection, despite the fact that big data analysis also takes place in terms of groups as (Taylor, 2017; Floridi, 2014). The role of anonymity in developing nations, particularly in non-democratic, authoritarian and oppressive regimes must also not be overlooked, as it is often vital for the well-being of those in marginalized groups (Ganesh, Deutch, Schulte, 2016). In data protection discourse, 'group privacy' is often neglected in favour of individual protection, despite the fact that big data analysis also takes place in terms of groups as (Taylor, 2017; Floridi, 2014). Inclusivity is required as target groups – such as those belonging to a particular religion or affiliated with a certain political party – are also at risk of identification. Often present in developing nations, and non-democratic areas, some examples include groups such as political activists, LGBTQ communities, people belonging of targeted ethnic backgrounds as well as those found in conflict areas. (Ganesh, Deutch, Schulte, 2016). Privacy, and the ability to stay anonymous may be crucial in these contexts.

The GDPR, on the other hand is only concerned, which may be sufficient in a European setting, but may be dangerous elsewhere. This lack of inclusivity is a significant limitation to consider, as it works against the improvement of privacy protection.

2.4 Market Monopolization

The discussion regarding what effect whether the GDPR will have on SME's in the context of big data, and whether it will improve or exacerbate the tech market monopolization is currently ongoing. While the vast quantities of available information provide opportunities for businesses, the inability to access this data is contrarily a competitive disadvantage. The majority of this data however is not controlled by governments or public bodies, but by private tech giants like Google and Amazon, or social media entities like Facebook (Alemanno, 2018). Being aware of the value of this data and it being a core element of their business model, it is also not probable that said corporations would be willing to share it. Primarily, while the GDPR aims to prevent both large businesses and SME's from collecting of data without individual consent, this could result in the opposite effect. According to Quantcast's report, the 90% majority of visitors to EU domains consent to GDPR and allow the collection of their data (Levin, 2018). Therefore, the tech giants who are more easily able to comply with the regulations are still collecting data unobstructed, smaller enterprises may find the new standards more difficult to meet. On the other hand, others state that the GDPR may decrease market monopolies, and level the playing field allowing SME's to compete (Alemanno,2018; De Hert, Papakonstantinou, Malgieri, Beslay & Sanches, 2018). Primarily, this could happen as a result of the transparent and limiting characteristics of the regulation – collectors are obligated to inform individuals which data is being gathered, and may only use it for those specific purposes. Further, this data has to be necessary, and retained for a limited period (European Commission, 2019). This way, a blanket regulation which sets the same standards on companies of all sizes and market control may better balance their opportunities.

While the focus of this blanket regulation is mainly on EU subjects, its global effects are global not something international and online businesses can afford to ignore. The fact that all parties now have to adhere to the same standards further has a number of significant implications for foreign businesses. American and Chinese companies, two dominant economic powers who are engaged in European markets may also be significantly impacted. The two currently conflicting opinions among scholars are that the regulations will either result in the superpowers' competitive advantage impaired, or their positions as market leaders solidified. Primarily, some say that due to the larger companies in the US and China being expected to expend large financial sums in order to meet the GDPR requirements, these costs may be transferred to consumers (Li, Yu & He, 2019). Additionally, as pointed out by Ruth Boardman, tech corporations whose business models center around data

collection - such as online retailers, media and financial businesses - will also be obligated to handle considerable volumes of requests for copies of personal information, as well as data deletion (Aliya & Murphey, 2018). SME's - companies with less than 250 employees - however, are exempt from certain obligations, such as the need for a Data Officer, or to possess exact documentation regarding the why and how data is being gathered (Clarip Privacy, n.d.). Thus, due to the costs associated with their large size, the competitive advantage could be decreased, allowing SME's easier entrance into the markets.

On the other hand, others have pointed out that the regulations may solidify foreign tech giants' dominant positions in the market. China in particular can be seen as an important outlier, as the majority of their digital innovation markets are based domestically, outside of the EU. This means that even while engaged in EU markets, the innovation processes will remain unhindered, which may allow them to become leaders in the data economy of the future. However, inspired by and modelled after the GDPR, China have also introduced what is commonly referred to as "the standard" - their own regulation called the *Personal Information Security Specification* (Sacks, 2018). With a few key differences that make the regulation less strict and more open to interpretation, the essence of its framework emulates and is highly comparable to the GDPR.

Thus far, the Standard, is not a mandatory regulation, although still considered a significant contributor to Chinese cyber security law (Li, 2018). Its objective is to protect private information, but while having many similarities to the GDPR – such as an expanded definition of what constitutes private information, the data minimization principle and a requirement for explicit consent- has much more relaxed requirements. However, although based on the European regulation, the fact that the Standard isn't mandatory, as well as its inconsistency with China's concept of a social credit system (which relies on private data collection and excessive surveillance), makes its effectiveness somewhat questionable (Campbell, n.d.). Such inconsistencies are further demonstrated by the current 5G network debate, and discrepancy between the privately owned company 'Huawei' and the Chinese government (Elten, 2019). While the corporation is said to be willing to comply to European privacy regulation, the government, which has a history of surveillance and spyware use, has not provided the same guarantees (Robertson & Riley, 2018; Kendall, 2009). This silence may be due to the fact that if an agreement is made but then dishonored the nation would be at risk of an international dispute. As a result, the data security concerns are obstructing Huawei's entrance to EU markets (Elten, 2019). Nevertheless, the existence of these laws outside of the EU have a number of implications regarding the global effect the GDPR has had throughout the tech industry. Following GDPR's implementation, a number of other nations have also been re-evaluating legislation and adopting similar frameworks. Brazil, for instance, has implemented the GDPL - the

"General Data Protection Law" (Baxter, 2018; Monteiro, 2018). With extensive similarities to the GDPR, the law also includes cross-border jurisdiction, the right to be forgotten clause, allows the consumers access and more control of their data, as well as a requirement to alert data breaches and the appointment of relevant staff. This highlights the long-term impact the regulation has inadvertently had on data practices as well as public and corporate attitudes towards privacy. By setting such a standard, and taking control of what was a free, under-regulated data market Europe may have set an example, with other nations gradually following the lead.

Chapter 3: Methodology

The following chapter recapitulates the research question and sub-questions of this study, as well as describes the rational, sampling process and research design in further detail.

3.1 Research Design

The theoretical framework, and existing literature related to privacy and its regulations outlined in the previous section highlights a number of elements significant to the GDPR and its effects on businesses. Cultural differences, power and financial inequalities, and political disposition being some of these major elements. Therefore, in order to answer the research question, '*To what extent is the General Data Protection Regulation creating a fairer and more inclusive regulatory framework in the global digital economy?*' this study further poses the following sub-questions:
Sub-question 1: In what way could the General Data Protection Regulation affect technology enterprises outside the EU in terms of competition and innovation?
Sub-question 2: What are the underlying assumptions behind GDPR and how may they be culturally-biased?

As the study examines and aims to bring the cultural and social assumptions behind the GDPR to light, as well as understand the range of concerns and challenges which may manifest if the regulation is globally adapted, a qualitative approach has been used. The data set considered in the study is composed of a selection of reports, articles, blogs and academic papers concerned with GDPR and themes discussed throughout the literature review - privacy, data usage, innovation, and so on. As there is a number of conflicts, power struggles, and tensions within those themes, critical discourse analysis (CDA) was selected as an appropriate approach. Often utilized in media and cultural studies, discourse analysis "goes beyond the semantic content of the data," and uncovers the deeper underlying concepts, assumptions and beliefs behind what is being stated (Braun & Clarke, 2008, p.84). Further, through implied meanings and the constructive role of communication, critical discourse analysis is also used to examine existing power relations, and those who benefits from said power, in a systematic way (Machin & Mayr, 2015).

Further, it is important to note that the study is not a legal analysis but rather focuses on discourse in the media, and the messages that are communicated to the general public. Media coverage, reports, documents and academic papers - written for common individuals as opposed to legal professionals are used. Media facilitates and is a significant contributor to discourse, and can present information and meaning from particular perspectives, consequently impacting the perceptions of a topic. Therefore, analysing this type of data will help understand the way in which

attitudes related to privacy regulations are constructed, transmitted and normalized (Machin & Mayr, 2012; Braun and Clarke, 2008).

3.2 Data collection/Sampling

The data corpus for this study consists of 22 reports, whitepapers, articles and academic papers. It should be noted that while academic papers also serve as a basis for the theoretical framework, those included in the dataset were selected for due to their focus on the application of the GDPR, as well as for data diversification. Further, as a significant amount of speculation and discussion regarding the effects of GDPR took place leading up to the regulation taking effect, relevant articles (3 texts) that were published before its implementation, between 2014 and 2016 are also considered. This year range was selected because the European Parliament began actively considering the proposal to implement the regulation during that time period, starting in March 2014, and was eventually approving and passing it two years later, in April 2016 (Smith, 2017). Being a critical period in regards to the regulation, the topic was examined by scholars, tech companies and related media; consequently, a number of preliminary concerns were introduced and discussed. The remainder of the data consist of material published after the regulation came into effect. This data includes corporate reports and articles published by tech, or other relevant businesses, articles published by general news media, tech blogs, as well as a few academic articles.

These categories of media were selected in order to include a larger range and variety in terms of discourse and perspectives. As pointed out by Hall (1997), discourse, and the way ideas are communicated results in particular ways in which topics are addressed, and sometimes limits alternative approaches. Therefore, a wider variety of sources may deeper insight into the topics, and result in a more accurate and reliable analysis. For instance, corporate reports tend to approach topics at a certain angle beneficial to the company, but are usually written in a formal tone, and aim to appear relatively neutral. Tech blogs and opinion pieces found within general news media on the other hand, tend to be less formal and more outspoken regarding their theories, beliefs and perspectives. These diverse approaches will therefore allow for a more complete analysis regarding they views on GDPR and privacy, the assumptions are being made, as well as reveal the dominant voices and interests within the discourse.

A number of the reports and articles include information not relevant to the study, such as short reports about the authors or executives of a company, as well as factual information about the GDPR itself. Such information will be taken into account, but if deemed extraneous will be excluded from the main portion of the analysis. For example, in the case of academic articles, while the discussion and conclusion are particularly significant, sections such as the literature review and

methodology may not be necessarily relevant to this study's research questions, and will therefore be excluded.

3.3 Operationalization/Analysis

The qualitative data analysis will include four main steps derived from Machin and Mayr organized in a modified coding frame (2012). Primarily, a few close readings of the articles will be done in order to understand basic contextual elements and denotation. A basic, surface level summery of what is being said, as well as information about the author, dates, and geographical origin of the item will be noted. The second step will involve examining the connotation of the texts. Significant keywords and phrases will be highlighted and examined in order to reveal what is being communicated at the implicit level. This involves inspecting lexical choices, as well as elements such as overlexicalization, suppression, or structural oppositions within the data. The terminology and style – whether there are negative or positive undertones and if the text is formal or informal – used in throughout an article may reveal the sentiment, and therefore the stance and perspective being taken. The presence of overlexicalization – repetition or a same word or idea - may similarly indicate where an argument is being solidified or the reader is being persuaded (Machin & Mayr, 2012). In contrast to this overlexicalization, suppression functions in an opposite manner where the absences in the text may discern what is being avoided. Finally, structural oppositions are the juxtaposition of opposite ideas within a text (such as private vs. public), which assist in solidifying a specific point or, for example, implying the importance of a concept through the use of its opposite. As explained by Machin and Mayr, this type of close analysis of what a text connotes may reveal strategies used for discourse construction, as well as uncover the assumptions, power dynamics and ways in which the reader's perception is manipulated (2012). Thirdly, cultural references and intertextuality, which are particularly significant in context of the study will also be investigated. Finally, all the combined findings were interpreted, and the perspective of the article, discourse position, significant tensions and whom the discourse benefits discussed and explained (Machin & Mayr, 2012). An excel table, as shown below, was used for each article to systematically organize the analysis and allow for a comparison. As the analyses is complete for each text, the entire data set was explored as a whole, compared and links between the findings and existing literature drawn.

Table 3.3: Illustration of the analysis flow

Item: (article # and title)	
Detonation	A brief summery and main ideas of the text
Connotation	Language analysis (choice of diction, tone, formal/ informal, overlexicalization, suppression, etc)
Intertextuality	Note any cultural assumptions or references that are made / perspective take by the article/ any relationship or references to other texts or events
Notes	Interpretation, and significant elements which stand out

3.4 Method Limitations

In its essence, while qualitative research provides deeper insight and understanding into cultural characteristics, social tensions and diverse perspectives, it is by highly subjective. Therefore, as well as having a number of limitations that need to be considered, it is also often challenging to determine the validity and reliability of such studies.

Primarily, there are notable constraints within the data sampling process itself. While the sample size determined for the study is sufficient and there is no definite rule regarding sample size, the included information is limited due to time constraints (Baker, Edwards & Doidge, 2012). Ideally, data should be collected until the point of saturation. Another limitation to this effect is the fact that only documents in English were examined, because while translation software exists, it is oftentimes not accurate or precise enough, especially considering that language choices are particularly significant to critical discourse analysis. This language criteria limits the data. This is especially significant as the study involves examining cultural differences, and there could potentially be valuable perspectives that are unavailable due to this barrier. Moreover, the use of purposeful sampling in cross cultural studies gathers richer data, such sampling is sensitive towards bias (Brislin & Baumgardner, 1971).

Furthermore, in qualitative research, the researcher's existing knowledge, bias and reflexivity have to be underlined, as these have an effect on the data's interpretation (Silverman, 2011). While there is a lot of debate about the extent to which validity and reliability are applicable due to the nature of qualitative research, related limitations also need to be considered. Replicability, for example is not as significant as accuracy, credibility and transferability (Winter, 2000; Hoepf, 1997; Glesne & Peshkin, 1992). Therefore, while using critical discourse analysis will allow the replicability of the study's conditions and, most significantly, *result,* the internal validity highly relies on other researchers interpreting and categorizing the data in a similar manner. Despite the method is systematic, it will still be subject to individual interpretation. For example, a certain keyword may have one connotation to a particular researcher, but a completely different connotation to a researcher from a different culture, which could affect the understanding of certain textual elements. Therefore, it is important to consider pre-existing knowledge and perceptions throughout the analysis and interpretation stages of the study.

3.4.1 Sampling Limitations

Even though the majority European, as well as a significant amount of foreign business are affected by the GDPR, the regulation only came into effect fairly recently. The effects of the regulation are still in the process of emerging and being studied. Therefore, despite being actively

discussed, the currently available texts may still be limited. Furthermore, even when concerning foreign cultures, most of the publicly accessible reports and news articles originate from the larger international businesses. This may be due to a variety of reasons, such as level of interest or stake in privacy and data related discourse, financial availability or a wider audience or customer base, and therefore a more active presence in the public media. While these articles provide valuable insight, they mainly prove a western point of view, and do not necessarily consider other cultural perspectives.

Chapter 4: Results and Analysis

This chapter will analyse and discuss the results of the data. Following the process outlined in the methodology chapter, the article analysis revealed a number of perspectives, significant themes, and concerns. Further, as reflected in these findings, although this study used the discourse analysis method, it is approached in the context of the theoretical framework and research questions. Additionally, despite there being notable overlap amongst the topics, the most significant ones revealed by the data can be categorized into four central components – attitudes towards the GDPR, the effects of the GDPR on tech enterprises, assumptions underlining the GDPR, and stakeholder power dynamics. The chapter will therefore be structured based on these discourse elements, compare the findings to existing literature and serve as a basis for the following discussion.

In summation, the findings indicate that according to the media, the need for an improvement in privacy standards and data practices is becoming increasingly evident. Although driven by diverse motivators, such as consumer pressure, politics, or social issues, this perspective is not only present in Western, but also international texts. As discussed in the first section of the chapter, despite over a year having passed since the implementation of the GDPR, there is still uncertainty and mixed opinion regarding its effectiveness amongst the public. While its objectives, as well as the growing necessity for regulation is understood, there are still a number of concerns that need to be overcome. The second section examines the impact the GDPR has had on businesses in the tech market. According to the findings, while enterprises of all sizes that fall under the regulation will be affected to varying degrees, the biggest effect will fall on large tech corporations. However, the debate regarding whether it will be to the benefit of these businesses or not is still ongoing. Furthermore, long term, global effects which may have been triggered by the regulation, such as an apparent change in attitudes towards privacy and transparency, as well as concerns regarding innovation are also examined. Further, the penultimate section views the sample through the framework of culture differences, and the potentially biased assumptions which underline the GDPR. Considering these elements allows for an evaluation of how enterprises outside of the EU may be affected, as well as the feasibility of non-Western nations applying similar regulations around the globe. Finally, the last section of the chapter conducts a critical analysis of the data in order to highlight the power interests amongst the main stakeholders – the people, corporations, and governments - within the data practice discourse. A brief overview of the topics which contributed to the analysis can be found in the table below.

Table 4.0: Data topic and sub-topic overview

Main Topic	**Sub-topic 1**	**Sub-topic 2**
Digital Economy	Value of Data	
Technological Development	Need for Regulation	GDPR Effectiveness
		Developing Nations
	Digital Divide	Digital Literacy
		Legal differences
	Automation	
Privacy	Data misuse	Transparency
		Trust
	Cultural differences	
	Competition & Innovation	SME's
		GDPR as an Opportunity
Power and Control	Power Imbalance	Monopolization & Market Dominance
		Data Subject's lack of agency
	Transfer of Power to Individuals	
	Governmental Interest	Censorship
		Data Sovereignty

An examination of the article types (i.e. academic articles vs. blogs) has revealed a few notable, crucial differences in the way privacy regulation discourse was approached throughout the data. The academic literature took a formal approach to presenting the information, incorporating theory, literature, and empirical evidence through understandable, yet technical language. This resulted in a clinical, scientific view, although the subject was still approached through a particular perspective. In contrast, tech blogs and news articles were aimed towards a more general audience, and were written in a more simplified and persuasive manner. These studies used real-world, often extreme, examples in order to emphasize their points, as well as more colloquialisms and loaded language – specifically diction with strong connotations. Subsequently, these articles provided a more opinionated perspective, which made the power dynamics and conflict within the discourse more explicit. Finally, due to being aimed at a corporate audience, reports of such nature were presented through a business framework. Therefore, although being written in formal, but simple, language and presenting seemingly neutral information, a more economic perspective was taken. The sampling variety revealed the views and attitudes of the diverse social groups, as well as allowing for a deeper interpretation of the power interests within the discourse.

4.1 Attitudes towards GDPR

The findings in the data supported the view that due to digital world being increasingly intertwined in the real world, the GDPR, and similar digital regulations, are becoming more necessary. However, while the GDPR itself is perceived as a positive improvement in fulfilling this requirement, it is not yet insufficiently developed and as a result, while the objectives of the regulation are recognized, there is doubt and concern regarding its effectiveness. On the other hand, despite the issues which may hinder the regulation's optimal effectiveness in terms of data practice improvement, the GDPR could still trigger a variety of global changes, consequently having a long-term effect on technology enterprises worldwide.

4.1.1 Positive Intentions and Effectiveness

One significant discussion regarding the impact of the GDPR on technological enterprises prevalent throughout the data highlighted an apparent discrepancy between the regulation's intention and how effective it is in practice. While each article approached the topic of privacy regulation through a distinct framework, both the GDPR's potential and positive intentions were acknowledged throughout the majority of the data. For instance, when addressing tech businesses, it has been described as "a springboard for success" (Springman, 2018, para.15) through which companies may gain a competitive advantage, a "catalyst for change"(IBM, 2018, p.1) in terms of improving overall data and security practices, and a way of discouraging excessive surveillance and population control through data minimization and erasure (Toobin, 2014). Similarly, the transfer of agency to data subjects is another objective endorsed throughout the articles. "Granting users, the right to regaining control over their personal data is at the heart of the European General Data Protection Regulation" (Urban, Tatang, Degeling, Holz, & Pohlmann, 2018, p.19). This perspective demonstrates the general belief that data reliant enterprises could be positively affected by regulation.

However, while the authors speculated the regulation's impact and endorsed these positive outcomes, they were overshadowed by heightened levels of doubt in its effectiveness in practice. This opinion of the GDPR being ineffective in achieving its purpose may have risen due to a variety of reasons. Primarily, while the regulation could provide a competitive advantage, in order to benefit companies would be required to commit its core principles. "…the downside of regulation is that it sets a minimum standard" (Springman, 2018, para.8). Companies however have been perceived complying to the GDPR only to a level of sufficiency, and thus not reaching the potential to effectively improve their data or security practices. Similarly, there has been a resistance against data regulation amongst tech corporations which centre their business models around data usage.

Due to the language which the GDPR is comprised of, certain elements are open to interpretation. This can create loopholes that will allow businesses to avoid true compliance, further contributing to this obstacle. For example, as demonstrated in the data, a business may comply with providing requested data to an individual but make the information particularly difficult to understand (Porter, 2019). "…this proposed law has been languishing for over two years, mostly because of strong opposition and lobbying by tech companies and other powerful actors" (Privacy International, 2019b, para.7). Such resistance stems from transparency issues, and the lack of trust for corporations due to a public concern for privacy and a misuse of personal data. Transparency, such as providing comprehensive personal information, could place these concerns in the spotlight, and consequently discourage the public from allowing the use of their data. As questioned in a tech blog, "if some pop-up showed to seek permission of 'tracking personal data' from 100 companies you have never heard before, would you just get scared and close the tab or click 'yes'?" (Wang, 2018, para.13). It is likely that the consumer is unfamiliar and lacks trust towards with these third parties, such request may alarm and deter from allowing the collection of personal information. In this regard, due to a lack of trust towards these third parties, informing the public about vast amounts of previously unregulated data may be potentially detrimental to its effectiveness as a resource. Corporate avoidance of such unwelcome, potentially detrimental outcomes therefore results in heightened resistance to policy. This further indicates that companies have not truly changed their attitudes towards data and privacy, but are acquiescing due to consumer pressure, and will continue opposing future changes. Another barrier for effectiveness, which is also discussed in the theoretical framework, is the privacy paradox. "Consumers, for the most part, would only agree to share "personal info" if they can receive justifiable rewards or gain access to something they cannot live without" (Wang, 2018, para.15). In accordance with the paradox theory, despite alleged, widespread privacy concerns, a large percentage of individuals have been shown to opt-in to data collection in order to access content (Teads, 2018). So, while the GDPR aim to protect personal information, data-subjects are easily volunteer it rephrase-unclear sentence. Thus far there has also not been sufficient evidence to determine whether consumers have changed their behaviour after GDPR. The public's willingness to disclose private information in return for online services further questions the effectiveness of the regulation.

Finally, another major concern outlined throughout existing literature, is that the regulation is still evolving and despite being an improvement is not yet sufficient to have any significant, global effect. "...these companies, and the GDPR regulations that govern them, have a long way to go if they want to give us real control over our data"(Porter, 2019, para.19). This lack of agreement

demonstrates that of yet, it is not entirely clear to what extent the regulation's global application could create an improve regulatory framework.

4.1.2 A need for regulation

The increasing pace of technological change and development is another frequent point of discussion amongst both academics and the general public. Regulation, outpaced by this growth, is no longer sufficient, which often results in a number of societal issues. Therefore, as reflected by the findings, the necessity for appropriate regulation is becoming increasingly recognised.

> Data used to be much simpler. Gone are my experimental teenage years of collecting user information on a school website and storing it on a MySQL database hosted on my personal computer in my home office with nary a privacy policy in sight. (Crichton, 2018, para.4)

The internet has matured since its introduction with the digital world gradually becoming an integral part of both businesses and everyday life. Following the introduction of packet-switching networks, the Transmission Control and Internet Protocols (TCP/IP), and thus the standardization of communication protocols, an increasing number of individuals began populating the online world (Featherly,2016). This caused the internet's transformation from its early "Wild West" iteration which has no policy or legislation, to one resembling the real world and establishing digital boarders through a complex system of regulation which vary from nation to nation. After the commodification of data by corporations, while the uses, quantity and value of data increased, regulation to support the data market remains underdeveloped. The lack of sufficient policy consequently resulted in a number of issues, such as privacy violations, the misuse of data, and security concerns. Public concern regarding these issues, as well as a need for regulation were implicit within the results. For example, this is demonstrated in the following experts - "data is and must urgently become the hallmark of risk regulation" (Almeanno, 2018, p.184) and "…activists have indeed hit Google and Facebook with GDPR complaints mere minutes after the long-awaited privacy regime came into effect across the EU" (Wang, 2018, para.3). Such occurrence indicates both the demand and impatience for regulation that allows the public to regain control over personal information. Despite the current issues with the GDPR, its effort has been perceived as an improvement in terms of regulation, and positive progress for security and data practices. Moreover, as previously stated, by applying a blanket regulation on each of the 28 EU member states, the GDPR intended to not only protect personal information, but also harmonize the diverse data laws. Directives, such as the DPD which was previously in effect throughout Europe, differ from regulations as they set central objectives; Each nation may decide how to transpose and incorporate them into the law, whereas a regulation does not allow for any deviation (European Union, 2019; Bender 2018). While there are a number of criticisms, this harmonization is also acknowledged to be an ongoing process. "A second regulation,

the ePrivacy Regulation, is meant to complement the GDPR and complete the harmonization process" (Degeling et al., 2018, p.2). The proposed ePrivacy regulation, while having a lot of similarities to the GDPR would specifically be focused on confidentiality in electronic communications, ensuring privacy over messaging platforms such as WhatsApp, or Internet of Things devices (European Commission, 2018b; Forrest, 2018). This means unlike the GDPR, the ePrivacy regulation will additionally protect non-personal data. Therefore, communications such as emails and instant messaging, will also be required to adhere to the best available encryption standards to safeguard confidentiality. This acknowledgement that regulation is necessary demonstrates how the GDPR, whether currently effective or not, incited a global increased in discussion regarding privacy concern and data practices. Therefore, even if the regulation is currently insufficient, it may result in long term effects as it continues to develop.

4.1.2.1 Regulation in developing nations

The need for regulation is additionally perceived in the case of developing nations. As governance is determined to be necessary for responsible and effective innovation and technological development, this may be something these nations may particularly benefit from. Introducing a technology or innovation to a society which does not have appropriate regulation to manage issues which arise with such development was shown to cause disarray and complications. A notable example of such instance can be seen in China's failed attempt to introduce bicycle sharing platforms as a way of pollution and traffic reduction. The bike sharing initiative, proposed by municipal governments was adopted by the private sector, resulting in a rapid spread of these platforms and a flood of bikes within the cities. Unfortunately, regulation to support these systems was insufficient, which resulted in a number of issues, such as an oversupply of the product, and further congestion as the equipment was improperly parked and abandoned in crowded or improper locations. Further, as companies began failing, large graveyards of abandoned bikes were formed. While the initiative could have potentially been an opportunity for the Chinese government to become a global leader in climate change, the lack of proper regulation resulted in the opposite effect. (Huang, 2018; Taylor, 2018). "Other parallels can be drawn with similar business models and platform companies, such as the food delivery courier Deliveroo, the car-hailing platform Uber, and the home-sharing app, Airbnb, where governance is a growing issue" (Bukht, 2017, para.7). Potentially socially, and economically beneficial innovations may not function as intended, or as demonstrated by the bike sharing example, even cause substantial issues. To avoid this, regulation should complement and be developed alongside such technologies. The fact that nations outside of the EU have been encouraged to either emulate the idea behind GDPR, or rethink and improve existing regulation further demonstrates possible, long term global effects of the GDPR. However, due to the numerous cultural assumptions on which it's based, universally applying the law may be ineffective, and possibly even detrimental at

its current stage. “While developing countries can ‘learn’ from some of the experiences of developed countries, they would still need to design policies that meet their own needs and which fit their local setting” (Bukht, 2017, para.17). Such policies, when adapted to a local context could place “greater focus on regional and gender inclusivity, (Bukht, 2017, para.17)” for instance or aim to “reduce inequality and enable participation of the underprivileged in the digital economy” (Bukht, 2017, para.17). This can be ensured by regulation through providing various legal safeguards which guard data-subjects from being targeted or exploited, thereby encouraging participation. Therefore, while Europe may be the leader in setting a golden standard for data practices, if other nations decide to adapt similar laws, adaptations based on their needs and cultural particularities will be needed.

4.2 The Impact of the GDPR

4.2.1 Tech Giants and Monopolization

One other interesting perspective within the data regulation discourse in relation to the type of organizations that might be most impacted, is the regard for GDPR as an “anti- google” law. This label indicates the belief that tech giants like Google and similar large corporations are specifically targeted by the regulations, and will therefore be most affected. This initial expectation for the regulation “to stop tech giants and their partners from pressuring consumers to relinquish control of their data in exchange for services” (Wang, 2018, para.3), is referenced repeatedly. However, as the articles progress and begin discussing this on a deeper level, the sentiment abruptly shifts. “GDPR has been described as an anti-Google law, but […] the irony may be that the supposed losers may well turn out to be the biggest winners after all” (Crichton, 2018, para.14). This juxtaposition primarily highlights the issue of market dominance and monopolization - one of the central topics within data discourse. This market monopolization is consistently seen as a barrier to innovation throughout the results, stating that “control over personal data by tech giants is one of the main causes preventing competition and ultimately innovation” (Privacy International, 2019a, para.2). The preliminary stages of GDPR’s implementation brought attention to such concerns through inspiring optimism for a system that could potentially level the playing field within the tech market. As discussed in the theoretical framework, currently the majority of the vast amounts of available data is controlled and managed by tech giants such as Google, Amazon and Facebook. Regulations such as the GDPR may either exacerbate the issue, or bring more balance through governing such data practices and providing more individual control over information. However, the data indicated that while improvement was initially expected, currently the general consensus within the industry is that while large corporations will be highly affected by the laws, they are still likely to benefit and strengthen their positions. SME’s on the other hand are predicted to remain at a disadvantage as a result of the additional challenges imposed by the data policies, since apart from a few stipulations -

such as the need for a Data Processing Officer – the GDPR security requirements equally apply to all businesses which process personal data equally, including those with fewer than 250 employees (Clarip Privacy, n.d.).

> The funny thing is, analysts have universally agreed that Google, Facebook and their likes, exactly what the GDPR supporters want to target, will solidify their monopoly in the digital world with this added barrier. (Wang, 2018, para.3)

> There is growing recognition […] of the need to address the role of personal data in assessing market powers and the distortion of competition by companies like Facebook, Google, Amazon, and other tech giants. (Privacy International, 2019a, para.9)

> …the complexity around these data sovereignty laws ultimately benefits highly scaled service providers who can manage the nuanced regulations around these laws in an automated fashion. That means, ironically, that Google likely will win long-term on its cloud side, along with other major cloud providers like Amazon and Microsoft Azure. (Crichton, 2018, para.3)

As well as this tension amongst competing corporations within the market, power dynamics between data subjects and the businesses who use the data is another salient conflict. Primarily, since certain institutions are in dominant positions within the market, they have thus far been able to dictate and "impose conditions on users" (Privacy International, 2019a, para.4), often collecting excessive amounts of, and misusing personal data. Additionally, another related argument is that as the result of this data monopolization and marker control, the public's choices will become more limited as smaller companies and their ability to advertise are hindered. This further relates to the previously stated issue of the regulation not being sufficient to achieve its goals, since companies such as Google and Facebook "are applying a relatively strict interpretation of the new law," in order to avoid large fines, and consequently "setting an industry standard that is hard for smaller firms to meet"(Wang, 2018, para. 4). This discourse illustrates the extent to which both large tech firms and SME's may possible be affected by the GDPR in the long run.

4.2.2 SMEs and Competition

In contrast, concerns regarding smaller international businesses not being able to meet the demands of the European regulation, and having their ability to compete impeded as a result, are also found throughout the articles. According to an IBM report, "some organizations have spent more than USD 1 million to become GDPR compliant" (2018, p.1). While the financial challenges

seem to be perceived as the most apparent issue that may be encountered, examining these in detail highlights their extent. For instance, these companies might not possess the financial means to allocate manpower to GDPR compliance, but opt to “wait until Google or Facebook finish their work and follow their footsteps” (Wang, 2018, para.23). This delay in compliance may also cause fines, hindering SME’s even further. Small advertising businesses may be similarly affected. Since companies such as Facebook are now obligated to reveal all the parties the data is shared with, these players may choose to drop smaller advertising firms to decrease this disclosure list as a means to avoid discouraging consumers from opting-in.

On the other hand, forcing larger companies to comply to a blanket regulation, and therefore lead by example could also be seen as an advantage. Primarily, agreeing with the theories of the literature chapter, the data highlights the fact that existing laws within each nation around the globe are diverse and complex. “Startups and even Fortune 500 companies are in no position to be able to handle these complexities without significant assistance” (Crichton, 2018, para.11). The GDPR aims to harmonize these laws, at least across the EU, thereby somewhat simplifying the compliance process and levelling the field. Another benefit is the possibility that industry leaders within the technology sector will begin adjusting their privacy and data practices, and eventually business models, in order to take advantage of the opportunities these improvements present (IBM,2018). The rest of the industry will gradually start emulating these corporations, leading to positive long-term effects.

4.2.3 GDPR as an Opportunity

Within the findings, GDPR has been approached both in terms of its disadvantages such as the risks and challenges faced by businesses, and advantages – the opportunities and rewards. Results indicated that some of the larger corporations view GDPR as an avenue to developing effective approaches to data. “It would be a mistake to regard GDPR as a bad idea just because it exposes organizations to legal risk"(PWC, 2018, p.9). In this regard, scholars have indeed stated that increased privacy and network security can be used as a tool to heighten trust amongst the participants of the digital economy, which is a salient component for its success(Kleist, 2004). Described as the facilitator of online business, it can be understood as “the intention to accept vulnerability based upon positive expectations, (Rousseau & Sitkin, 1998, p.395)” hence a willingness to reply on an entity due to a certainty for a positive experience. Some contributing factors to amplifying this assurance include privacy policies, applicable protection frameworks, as well as network security (Kleist, 2004; Hemphill, 2002). Similarly, as discussed by Hemphill back in 2002, as well as personal privacy, a number of elements which are now present in the GDPR have also been identified as significant factors contributing to consumer trust in digital commerce. This includes the

honesty and transparency of a company in regards to data collection, the ability for a user to consent to or select what information is collected and for which purpose it is used, the ability to view what data a business holds, as well as the available security measures against unauthorized data use (Hemphill, 2002). Further, as well as enhancing trust, data and network security technologies may simultaneously reduce the interpersonal variable, which may be suitable for larger corporations that are often perceived as more impersonal and not humanized to the same degree as their smaller counterparts. Humanization of corporations was shown to plays a significant role in brand trust (Beck & Prügl , 2018). The heightened privacy and security requirements imposed by the GDPR may therefore serve as suitable method for trust building for entities that are unable to connect with their customers on a more personal level. Moreover, as there was previously a lack of incentive, for a lot of organizations information management remained an "underdeveloped part of the technology stack" (PWC, 2018, p.10). The regulation provides this incentive as well as opportunity for enhancing customer relationships.

Additionally, as a result of recent privacy scandals and events such as the Snowden disclosures, consumers began expecting more responsibility from the entities who collect and store their personal information. The requirements imposed on these corporations by the GDPR highlighted such privacy shortcomings, while also providing businesses with a cost justification for improving and developing their data management systems. Consequently, if the core intentions and values of the European regulation are embraced by the industry leaders and large international corporations, this may become the "catalyst" for improving standards across the board. To this effect, as reported following IBM's survey, 39% of businesses within their sample "saw GDPR as a chance to transform their security, privacy and data management efforts, and 20 percent said it could be a catalyst for new data-led business models" (2018, p.4). As well as demonstrating a possible manner in which the regulation may incite a new global standard for privacy and data practices, this view reflects our technological evolution and need for the further development of appropriate regulation. However, while this is a positive and ideal outcome, one criticism that can be made is that all companies are assumed to be free to compete in the market, as well as have the sufficient financial means to comply with the original regulatory requirements.

Moreover, the regulation was initially perceived as 'punitive' against major corporations whose business models heavily rely on data usage; However, as the GDPR was implemented and these same businesses began the compliance process, the mindset shifted to consider "security and privacy as key business differentiators (IBM, 2018)," emerged. As the mandatory regulation was implemented and compliance became inevitable, businesses could take the obligations as an opportunity to significantly improve their practices, and as a result leverage a competitive

advantage. As expressed in the results, "businesses often have vast amounts of data stored in silos which are disconnected and difficult to reach, or have databases with significant amounts of redundant, obsolete, and trivial data"(Kemp, 2019, para.5). Eliminating such unnecessary systems are an example for which the regulation may be used as the incentive to revise their data handling, making previously stagnant systems like data storage more efficient.

While these reports are mainly concerned with tech giants and industry leaders, media from smaller organizations outside of the West has also noted changing attitudes towards privacy and disclosure within the business sector. These reports identify major global events, like the previously mentioned Edward Snowden scandal, as the primary triggers for the public, and subsequently the businesses, to become concerned with data issues. Transparency reports, for example, used to be regarded by businesses as a specialized interest and a liability that could potentially attract negative media or governmental interest. “The Snowden disclosures about government surveillance, changed the transparency landscape” (Budish, 2017, para.3), however, and brought privacy concerns into the spotlight. “Catalyzing events seem to be necessary to accelerate the acceptance of transparency reports” (Budish, 2017, para.6) - while non-Western nations, particularly countries in Asia did not yet experience an event of a similar scale to the Snowden scandal, “smaller events have had a clear impact”. Data scandals and general security issues, even though not as prominently covered by the Western media, are indeed similarly widespread throughout the globe. In 2016, as a means to call for higher security standards, a hacker group in the Philippines has gained access and ‘vandalized’ the ‘national Commission on Elections’ website, leaving millions of voters’ data vulnerable to the breach (Bueza, Manuel, 2016). Singapore has similarly experienced its largest healthcare data leak when the private information of 1,5million patients was exposed as a result of another hack in 2018 (Yu, 2019). In India, thousands of confidential Aadhaar numbers - identity numbers that are attached to names, biometric data, and partial phone numbers – were leaked due to negligence of the authority responsible for securing the information (Whittaker, 2019). Increased awareness, as a result of controversial events, has influenced attitudes towards issues related to privacy and disclosure amongst the public, consequently creating a demand for better control of personal information, and improved security standards.

4.2.4 Privacy and Innovation

The tensions between privacy regulations and innovation are a central subject within privacy literature, however currently does not appear to be a significant concern amongst the public media. While it is frequently referred to, only a minority of the sampled articles elaborate, or discuss this conflict in detail. “What we need is a guiding principle in designing regulations for those emerging technology. It should be designed in such a way that it will not hamper creativity and innovation in

tackling societal challenges" (Agahari, 2018, para.8). Nevertheless, a few interesting findings did emerge from the data in regards to how the GDPR is perceived to have affected innovation. Primarily, the constraints created by the regulation are viewed as a 'stimulus for innovation' (Springman, 2018, para.5) that would force organizations into being more creative and resourceful in their everyday operations. This perception is accordant with the theories discussed in the literature review which frame regulation as an opportunity for innovation (Zarsky, 2015). The previously discussed market monopolization posing a barrier to innovation, is also consistent with the assessments of the theoretical framework and repeatedly expressed throughout the data. Interestingly, a common attitude towards innovation implies that all innovation is always positive and beneficial. This is a fundamental assumption amongst those arguing against privacy in favour of supporting innovation, both throughout the public media and theoretical literature concerning privacy and data. Due to the strong, social association that innovation has with improvement, this pro-innovation bias is the belief that innovation is universally beneficial, should be rapidly applied (Rogers, 1995). In reality, adopting certain innovations may either not have a significant advantage, or may even be detrimental in certain situations. An example of this is the introduction 'loot boxes,' a mechanism where a player may use real currency to purchase and open a virtual crate containing random in-game items, to the gaming industry. For the industry, this feature dramatically increased revenue, but has also been linked to gambling addiction (Macey & Hamari,2019; Zendle & Cairns, 2018). While there are advantages of innovation, contextual adaptations need to be taken into account as it may not always have beneficial effects across all situations or communities. The previously discussed introduction of bike sharing platforms in China another relevant example. While it is an extremely innovative solution in regards transport and other issues such as vehicle emissions, the scheme backfired as the competitive nature of these platforms, and lack of regulation was not taken into account. While innovation is necessary or improvement, some technologies or business practices may not automatically be good for certain communities, therefore favouring it above privacy, as is often the case in data practice discourse, might not always be appropriate.

The concession that privacy and innovation may be able to coexist without being mutually exclusive, however, is one of the most interesting and significant observations identified within the results. A privacy conference report published by CMO.com (Nuttley, 2016) for instance, identifies multiple experts emphasizing this opinion:

> It's not privacy or innovation—it's privacy and innovation. The personal information economy can be a win-win situation for everyone. Get it right, and consumers and businesses benefit. Consumer trust is essential in driving growth. - Elizabeth Denham (para.3)

> The debate about data is framed as a balancing exercise, […] we want to use data to power growth. We also want to protect rights and trust, but more of one means less of the other, which seems an undesirable trade-off. Can we find a way that growth sustains privacy and trust, or even creates a mutually reinforcing cycle?" - Stephen Deadman (para.5)

Although this appears to be a relatively recent attitude, this is finding is significant as it further illustrates a steady change in stance towards privacy and data practices, as well as the way in which they are approached. Such changes are further strengthened by regulations such as the GDPR and may collectively work towards setting new global standards within the tech industry. Further, if privacy is no longer viewed as an obstacle to innovation but rather a co-existing, lateral system, there may be less resistance against policy and legislation from major corporations. This could potentially not only allow regulations such as GDPR to thrive and succeed in improving data practices, but also encourage a better relationship between businesses and data-subjects, thereby benefiting competition and innovation in the long run.

4.3 Assumptions Underlining the GDPR

The theoretical framework on which the main research question is based has considered the probability of numerous assumptions underlining the GDPR, some of which may be culturally biased. Attitudes towards privacy, data equality, as well as an understanding of digital information and the manner in which the relevant technologies functions are some requirements for the optimal application of such regulation. Comparing the sampled article types revealed several differences in the degree to which such assumptions were made or acknowledged.

Corporate reports which concerned data and privacy practices mostly approached the issue from a business, financial perspective. Often B2B in nature, these appeared to be written with the intention of encouraging other businesses in the industry to accept and embrace the regulation, and as a result supressed, and avoided referring to any related limitations or challenges. Throughout the reports, when discussing the GDPR, its potential to improve global security standards was often highlighted, however no social barriers, cultural differences or digital inequalities were addressed. In contrast, articles that were written in a more academic manner demonstrated a critical awareness of cultural differences. This awareness is demonstrated in a number of ways, such as critiquing a study's limitations of a research, or through a strong emphasis on the scope of the research - repeatedly accentuating the fact that a finding is specific to Europe. While these were mostly focused on analysing empirical evidence for direct effects of the GDPR, and the scope of these articles was not relevant to these specific limitations, they were still noted to some extent. Finally, there was a level balance amongst blogs and news articles between those who addressed such

issues and those that did not. Unsurprisingly, authors who took an interest in, or originated from non-Western sources, paid particular attention to cultural assumptions and limitations, for instance acknowledging economic differences and variation in education. This was expected as such challenges and topics are much more relevant to "the Global South" and developing nations, the majority of which are located outside the EU. Further, these authors adopted a more comparative style where both the Western, and non-Western were considered, providing a broader perspective.

Cultural differences, and the separation of nations are important to consider as in reality boarders are significantly more difficult to maintain within the modern information economy. Businesses, compete within international markets, and as a result, the majority of new business models within the tech industry aim at an international consumers (Taylor & Fosler, 1994). The flows of data are consequently transnational in nature. Therefore data, without proper network security and protection is globally vulnerable, as breaches can originate from any location. The GDPR may be an initial step towards setting an improved framework for security and privacy practices within this global digital economy.

4.3.1 Privacy as a Basic Human Right

A Western perspective and understanding of privacy, its value and importance are implicit within the discourse, although often not acknowledged directly. This can particularly be observed in the portrayal of privacy as a fundamental human right, which is a primarily European concept. Unsurprisingly, this perspective was mainly expressed within data from either International or Western sources, while those from Asian regions, for example, focused on data and privacy discourse in terms of development, regulation, or politics explain. Further, differences between national views of the value of privacy were also highly evident in articles concerning the United States; as certain elements within the GDPR – such as the right to be forgotten – clash with the current US legislation, the contrasting values resulted in heighted debate.

> In Europe, the right to privacy trumps freedom of speech; the reverse is true in the United States. Europeans think of the right to privacy as a fundamental human right, in the way that we think of freedom of expression or the right to counsel," Jennifer Granick, the director of civil liberties at the Stanford Center for Internet and Society, said recently. (Toobin, 2014, para.7)

The legal differences illustrate some of the challenges that may arise if regulation were to be globally applied, and highlight just two diverse perspectives. Outside of the West, if a regulation like the GDPR were to be universally applied, it would be facing even further challenges due to further diversification of laws and cultural.

4.3.2 The Digital Divide

The reflection of social inequalities in the online world is another salient topic that is frequently recognized and discussed throughout the articles. These digital inequalities are expressed in relation to a geographical division within the digital economy and distribution of information – "the global south" and north divide of developed and underdeveloped nations. The data "might not cover the so-called "data invisibles", i.e. those people who, generally due to their socio-economics, are not counted or tracked within the formal or digital economy" (Almeanno, 2018, p.184). This refers to those "at the bottom of the pyramid who live below the poverty line," (Bukht, 2017, p.16) such as immigrants, women and children, those residing in impoverished areas. Essentially, the marginalization in the offline world is often reflected in the digital economy, as individuals who struggle to afford basic necessities may not have the income to access certain digital services. Furthermore, this divide may also be identified on a smaller scale, as a local divide within a particular nation itself. An example of this is Indonesia, where the majority of citizens are considerably active in the digital world, with their mobile devices outnumbering the population. However, the nation still "face a significant challenge in narrowing the digital divide. Around 77 per cent of internet users are centred in Java and Sumatra, and less than half of citizens in eastern part of the country do not have access to the internet" (Agahari, 2018, para.3). One of assumptions underlining the GDPR, as well as the theoretical concept of applying such regulation, is the expectation of a homogenous distribution of data. The limitations and inequalities of data distribution are disregarded, which might exacerbate the divisions within the data economy. Additionally, if the EU leads other nations by example, and similar regional regulations are adapted, what used to be a borderless internet where everyone has access to the same information would no longer exist. The digital divide could reshape to not only include economic and geographical separations, but also those caused by legislative restrictions.

> …policies in developing countries need greater focus on regional and gender inclusivity and other technical and social issues to reduce inequality and enable participation of the underprivileged in the digital economy. Regulatory reforms are also needed that ensure platform operators' responsibility when it comes to protection of users against exploitation and hazards. (Bukht, 2017, para.17)

The findings indicated that narrowing this digital divide is a significant issue, and would require regulation designed and customized specifically to the context of these developing nations. While the GDPR may be beneficial in the EU and represent an improved standard for data practices, it is culturally bias. The issues which developing nations confront are not considered by the regulation, therefore making it inadequate for application in such regions.

4.3.3 Digital Literacy

Similarly, to these issues with online representation, the GDPR, tech sector and online world, are reliant on the assumption of adequate digital literacy in order to function effectively. The importance of literacy and understanding is even indicated in the outcome of GDPR's transparency requirements. It was shown that the regulation succeeded in improving the way policies and privacy notices were presented to the general public. Before its enforcement, as stated by one article, it would "require a college degree to actually understand" the majority of such policies, whereas the currently simplified terminology resulted in a more "positive effect on web privacy (Degeling et al., 2018, p.14)". However, while it is important to recognise that this transparency requirement demonstrated the consideration for digital literacy issues and represents a significant improvement, the magnitude and complexities within the modern tech sphere still lack understanding. For example, when considering the constantly evolving data systems, it becomes evident that comprehension of the way in which they function is limited amongst the public.

> It is already difficult, if not impossible, for a data subject to understand or control how many entities hold what kinds of data about them, how they are linked, shared and aggregated. Consumer tracking is no longer limited to browser cookies that individuals can block or delete, but has advanced to more sophisticated techniques, such as cross-device tracking and device fingerprinting, which are much harder to escape. (Privacy International, 2018, p.8)

Modern technology thereby exposes a significant limitation to digital literacy, as this concept suggests an exhaustive understanding of data systems, including the collection process, amalgamation of the information, as well as its distribution. However in reality, innovation and new technology often introduce a number of unintended consequences, and unexpected effects on the users. Moreover, another similar limitation is that within the idea of digital literacy, the obligation and responsibility of being informed is placed on the individuals. While such knowledge is certainly advantageous, individuals may be severely limited in exercising their will in certain parts of the world, particularly non-democratic nations. This is particularly significant as while there has been a notable decline of democratic nations over the past decade, authoritarian powers have been growing (Freedom House, 2019). As per their national laws, such authoritarian powers could force corporations to provide them with personal data. The 'Blasphemy Law' is, for example, aims to find and punish those speaking out against anything that is considered sacred, such as religion (Kelly,2018). In 2017, a study identified 71 countries have such laws penalizing speech, some more severe than others – Iran and Pakistan, which are more authoritarian, for instance carrying a death penalty for such an infraction ('Ranking countries", 2017). Private data collected by businesses could

potentially make it extremely simple to identify and locate individuals breaking these laws. Even in developed nations, as demonstrated by transparency reports often provided by corporations, governments may request a business such as Facebook to share user data for legal purposes (Twitter, 2019). Therefore, there is a limit to media literacy, as the will of an individual in terms of privacy is not necessarily always adhered to.

The GDPR is largely based on the concept of allowing data subjects more control over their own data and what it is used for. This is further based on the assumptions that the subjects – the general population – are aware of, and understand their rights, what the data is used for, as well as having basic knowledge of how the relevant technologies function. However, as discussed in the theoretical framework, the levels of digital literacy are not homogenous, and this is therefore not always the case. "…even after the GDPR will have come into force, individuals will not always be aware of their rights and of the forms of redress that they have available" (Privacy International, 2018, p.17). Those on the other side of the divide, for example, and not as active in the digital economy might not have the same level of understanding regarding data practices as European subjects. Topics related to more complex systems such as profiling and automation appear to particularly lack concrete comprehension both by the public and industry. This is notably reflected in regards to machine learning. It "can be difficult, even for the designers of such systems, to understand how or why an individual has been profiled in any particular way, or why a system has made a particular decision" (Privacy International, 2018, p.8). While being an extreme example, this illustrates how even the architects of these systems are not entirely clear on how they function, therefore it is unreasonable to expect sufficient understanding from the general public.

Additionally, according to the GDPR, controllers may deny requests for information or deletion if a data subject cannot be identified based on the information. If the data does not breach privacy, it may be used unhindered. However, this becomes more complicated when it comes to automation and machine learning, as a lot of information, whether accurate or not, can be inferred and predicted (Privacy International, 2018). This issue further demonstrates how regulation, including the GDPR, is still not sufficiently developed to effectively manage modern technologies. Consequently, businesses and organizations that rely on automation, artificial intelligence and machine learning may face further challenges in the future.

4.4 Power: People, Government and Corporations

The following section will discuss the power dynamics within the data and privacy discourse. Results indicated three salient stakeholder groups - the data subjects, corporations and data controllers, and governmental bodies. The regulations impacted each of these stakeholder groups through a shift in their power dynamic; Individuals were given increased control over their private

information, businesses and corporations became more restrained, and governments obtained a degree of data sovereignty. Thereby, the findings revealed the effects the regulations had, through this shift in the power dynamic, on each stakeholder group. Understanding the interaction and relationship between these stakeholders reveals the extent to which organisations may be affected by GDPR's regulatory changes. As discussed in the literature review, data has become an increasingly valuable commodity in the eyes of corporations, and subsequently governments. As a result, data represents money, and power. By enforcing data-practice restrictions on businesses, and redistributing data control amongst the players, the corporations' previously uncontested ability to dominate, use and profit from the data is decreased. Consequently, as enterprises are affected by these types of data regulations, the way in which they compete and innovate will also change.

4.4.1 Data Subjects: Transfer of Power

In line with existing literature, the findings demonstrated a power imbalance between the data subjects and data collectors. The tension arose as a result of the commodification of private information and data, as well as their growing value. Increasingly, the consumers' helplessness and lack of agency has been becoming an evident concern, which is repeatedly expressed, both directly and indirectly throughout the data. Lexical choices and connotation played a particularly significant role in communicating these issues. For instance, using language such as 'victims,' and 'violators,' throughout the discourse, as well as referring to the inability to 'escape' online records implies powerlessness and a lack of control. Other phrases such as " the business models of companies in dominant positions which can impose excessive collection of data on people who have become "captive users" (Privacy International, 2019a, para.4), and "[photographs] spread across the Internet like a malignant firestorm," (Toobin, 2014, para.2) similarly illustrate this in a more direct manner. Understanding who uses the data-subjects information, and how it is used is repeatedly described as 'difficult' or even 'impossible' in context of the modern tech industry. Furthermore, throughout the data, large corporations and tech giants such as Google, Facebook and Twitter were specifically identified and accused of being the perpetrators of this conflict, and the ones responsible for misusing private information. Indeed, these large, international corporations have become infamous over the past decade both as a result their aggressive market dominance and problematic data practices. Such allegations by the data subjects not only emphasize the conflict between individuals and the companies, but also the identify these tech giants as a central target of privacy regulation. Consequently, the perception that the GDPR has been created as a direct response to the misuse of information and large tech corporations further contributes to GDPR's reputation as an "anti-Google" law. This reputation is not surprising, given that while the number of incident reports and investigations is high, the public is mainly aware of the high profile cases and entities –

such as Google, who have had to pay a fine of approximately €50 million (Hill, 2019; Lovejoy, 2019; Porter, 2019). In accordance with the way this power conflict has been perceived, generally the data indicated approval of the GDPR in terms of allowing the public more control over their own data.

However, a point is also made that while regulation provides the necessary tools for controlling one's individual data, the responsibility to take action is also transferred on individuals. "Modern data protection laws like the EU General Data Protection Regulation recognise the right to data portability, and demand that individuals must be given the tools to be in control of their data" (Privacy International, 2019, para.8). Some authors go as far as to imply that these data issues arose as a result of the public's negligence in safekeeping private their private information. "Thanks to [...]our acritical generosity in giving away so much persona information, these companies know more about us than our partners and closest friends"(Almeanno, 2018, p.183). Consumers, whether or not being aware of the risks of publishing private information, were primarily responsible for becoming a data subject. This another problematic point, since social media has become part of the public digital sphere where users have a right to visibility through sharing data with a trusted platform. There is no expectation for this data to be clandestinely shared with or sold to unknown third party companies. As previously discussed, the regulation is based on a number of assumptions, such as differences in privacy perception, digital literacy, and a general lack of understanding data practices. These assumptions may similarly have an effect on the degree to which these newly available tools will be utilized. Other factors, such as the privacy paradox, or simple disinterest could also contribute.

4.4.2 Corporations: The Value of Data

Through benefiting individuals by providing more power, the GDPR simultaneously threatens that of large corporations. As discussed in the theoretical framework, data is now considered a valuable commodity, which corporations want to keep control of to utilize for gaining a competitive advantage. Through transferring power to individuals, the GDPR redistributes control over this commodity, which is perceived by these companies as an undesirable outcome. This negative perception is demonstrated by the concerns regarding the GDPR's effectiveness as discussed earlier within these results, as it was partially based on the resistance large corporations showed against data and privacy regulations. The power conflict between the corporations and data subjects is further demonstrated in the social pressure organizations appear to be under. "Clearly, consumer privacy is something that companies can no longer dismiss as unimportant" (Silber, 2019, para.5). This shows how much effect data subjects, who previously had no control over their data, had on governments, and consequently – through privacy legislation – on data controllers and corporations.

> In subsequent years [after the right to be forgotten clause was first carried out], the E.U. has promulgated a detailed series of laws designed to protect privacy. According to Mayer-Schönberger, “There was a pervasive belief that we can’t trust anybody—not the state, not a company—to keep to its own role and protect the rights of the individual.” (Toobin, 2014, para.11)

Such lack of trust in corporations using data responsibly may have been caused by major events, subsequently causing the stakeholders to acknowledge that "far too often, data protection is an afterthought"(PWC, 2018, p.6). According to the results, this justified attitude contributed to the social pressure for an increase in data rights. This further highlights the power conflict in data and privacy discourse. However, as evidenced by the opportunities perceived by certain market leaders in regards to the GDPR, corporate resistance may be slowly decreasing in favour of using the regulation as a means to a competitive advantage. “ ‘…the individual needs to be at the centre of the discussion.’ This is because individual agency is a driver of growth” (Nuttley, 2016, para.40). Based on these results, this conflict may therefore be interpreted as advantageous to both stakeholders – the data subjects and data controllers - and the GDPR as a potential solution – allowing individuals increased control over their data, and providing corporations with the incentive for an improved business model.

4.2.3 The Governments

The final stakeholder of the power conflict within privacy discourse that may benefit from increasing control over data practices are the governments. This governmental interest was frequently expressed in the findings; however, the majority of the data sample was of corporate or civilian origin and concerned with either an academic, business, or technical perspective. “[Data has become a] tempting target for law enforcement and intelligence agencies. Through various investigatory powers, these government agencies can demand that social media companies, e-mail providers, ISPs, and other intermediaries turn over sensitive records and message content” (Budish, 2017, para.1). Therefore, as the scope of the sample excluded legal and governmental documents the results may be biased in representing this stakeholder. Nevertheless, civilian and corporate perspectives provide valuable insight into further concerns and potential issues in regards to data practices. From the perspective of the articles, a government can misuse the GDPR, or any similar data regulations, to impose governmental control by means of censorship or to ‘colonize’ and profit from the digital data economy. “That free market in data is rapidly disintegrating as governments increasingly take an interest in data, not just for privacy reasons, but also for population thought

control and economic growth purposes" (Crichton, 2018, para.5). These governmental interests may therefore significantly impact technology enterprises both within and outside the EU.

Primarily, it is important to consider that a regulation such as the GDPR, and dynamic it creates between the people, corporations and governments may not be a significant concern in a Western, democratic nation. However, as pointed out in the theoretical framework, perpetrators in non-democratic, authoritarian nations could use such laws as a means to justify censorship. "[The] fears of many in the industry that the 'right to be forgotten' will be abused to curb freedom of expression and to suppress legitimate journalism that is in the public interest" (Toobin, 2014, para.26). These concerns indicate that just as there are apparent issues of trust between the data subjects and corporations, similar tensions exist between the subjects and governments. Moreover, the fact that nations outside of the West have diverse regimes and systems of government is further highlighted, which is significant as the GDPR, being specifically designed for Europe, does not account for such variation. Such culturally bias assumptions, as discussed in the literature, problematizes the global reach of the regulation.

Secondly, another salient point within the discourse relates to the impact privacy regulations may have on the free data market within the digital economy. As governments take an interest in the data market, privacy legislation may allow them more control within their geographical boarders, and in the case of GDPR, beyond said borders. Thus, through these regulations, a nation has the ability enforce its own laws in foreign jurisdictions. As the EU now has authority over its' data subjects' information, if other nations take example, what used to be a free flow of information within a 'borderless' internet will become more 'colonized.' "While the European Union's GDPR regulation has gotten the most press (probably because of the several dozen emails you received about it), the EU is hardly the only government enhancing its data sovereignty" (Crichton, 2018, para.7). Concerns regarding such division is expressed throughout the data: both implicitly, through presenting Europe as the leader of data practice innovation – implying that others will follow – as well as directly highlighting examples of similar regulations inspired by the EU. These laws […] all serve the same purpose — to bring data back home and ensure that the desires of a country's people (and, of course, its leaders) can be imprinted on how that data is used" (Crichton, 2018, para.8). These findings of data colonization, and data sovereignty are also in line with existing literature on this topic, and further demonstrate the impact the regulation may have had on enterprises outside the EU.

Lastly, in addition to having increased authority over their data subjects' information, governments may further economically profit from data regulation. The fines imposed on non-compliant corporations who do not meet sufficient security standards or misuse data will primarily

allow governmental stakeholders to profit from the digital economy. While seemingly a minor benefit, this will provide a significant advantage and control over previously unchallenged powers, such as industry leaders and large, international tech enterprises. Moreover, as previously mentioned, the commitment to improving data practices as a whole may provide social and economic benefit overall – both through developing security and data practice standards, as well as creating potential opportunities for companies to gain a competitive advantage and build consumer trust. Additionally, this may further provide both social and economic benefits to those governments in which national companies leverage the potential opportunities and competitive advantage.

Chapter 5: Conclusion

This section will recapitulate the findings presented throughout chapter 4, discuss their implication, as well as answer the sub- and main research questions. The primary goal of this study is to explore how the GDPR may have affected enterprise outside the EU in terms of innovation and competition. This is achieved by critically analysing privacy discourse in context of the regulations' effectiveness, types of organizations that are most impacted, and issues or assumptions on which the laws are based. Lastly, the study will acknowledge the theoretical and practical limitations, as well as make some suggestions for further research.

5.1 GDPR's Impact

Primarily, it is important to reiterate the uncertainty and lack of clarity amongst the scholars, authors, and public media regarding the degree to which the GDPR may actually be effective. Despite being implemented over a year ago, the regulation is relatively new, still being developed, and has yet to address several issues which hinder it from achieving its objectives. Similarly, based on the results, the regulation has seemingly began inciting global, long term changes that are still in the process of fully manifesting. Nevertheless, lest the GDPR indeed results in causing sufficient impact, its scope and severity has invited significant debate and investigation within privacy discourse since its implementation.

According to the results, all international organizations which are to some degree reliant on data use within their business models will undoubtably be impacted. However, the considerable influence will most likely be received by the large corporations, tech giants, and industry leaders. The dominant players of the digital economy, which are in most cases financially secure, may solidify their positions, as they have means and manpower to rigorously interpret, and comply with the requirements. While being to the benefit of such enterprises, this would result in increased monopolization and decreased competition. This exacerbated power disbalance would consequently worsen the conflict between the stakeholders, as well as hinder small enterprises. On the other hand, as tech giants such as Google are currently primary focus of the governments, and regulation enforcement is limited, SME's might be overlooked, allowing them sufficient time to comply, and therefore not be negatively affected due to finical issues. Similarly, if the GDPR achieves the objective of a more even distribution of the control over data amongst the players – SMEs, tech giants, governmental bodies, as well as data subjects – this would encourage competition and innovation as a more consumer-centric system is developed. Industry leaders may accept and even adopt the values of the regulation, resulting in improved business models and a shift in attitude

towards privacy and innovation. This is particularly important in context of large corporations that have an international presence, as an adaptation of such values may cause their export to other non-EU, non-Western nations. Consequently, this can improve the global standard in terms of privacy and security.

Assumptions which may be underlining the GDPR, especially those that are culturally bias are another crucial element that may influence how enterprises that do not share EU values, or are in divergent social conditions, may be impacted by the regulation. Issues brought up both in the literature and results, such as literacy, data invisibles and the digital divide are a significant obstacle to effectively applying the regulation and setting a global standard. Further, as the online world has presently been hypothesized to reflect real life inequalities, applying such a privacy regulation may even exacerbate current disbalance and segregation within the digital economy. This in turn may negatively affect enterprises outside the EU, particularly those within developing nations. Moreover, as a large portion of the population is excluded, this may in turn affect the competition and innovation within those regions. However, while such assumptions have not been taken into account by the legislators prior to GDPR's implementations, they have been the subject of active debate within the industry. As a result, further iterations, and developments of the regulation may be improved in consideration of these concerns.

Findings indicated a number of ways in which the GDPR could affect technology enterprises outside the EU in terms of competition and innovation, some of which have already began developing. Most importantly, the regulation (and privacy conflicts which resulted in its creation) has encouraged other nations around the globe to examine their own approaches to data practices, and in certain cases even adapt similar laws. These revisions indicate a fundamental change within the tech industry, and long-term effects produced by the GDPR. This may further stimulate a change in attitude towards privacy practices, resulting in more data, and security conscious business models. These enhanced security standards may consequently improve trust, and relationship between corporation and consumers. This may provide a competitive advantage for certain businesses, and benefit society as whole through a decrease in the misuse of data. Similarly, according to the findings 'advanced' nations are considered leaders in establishing standards; developing nations could be inclined to imitate their frameworks. As discussed in chapter 3, some have indeed already done so. Regulatory reform would provide a number of benefits as these nations solidify their positions in the digital economy, including the prevention of exploitation of related systems (such as data abuse), autonomy of private information, and laws specifically catering to modern business models. Competition and innovation may also develop based on these adjusted models.

As regulations such as the GDPR are passed and enforced by governmental bodies, this is another powerful stakeholder group within the results which has a significant effect on competition and innovation. Primarily, as discussed in chapters 3 and 4, the regulation can be viewed as a tool for centralizing data control, establishing data sovereignty, and as a way of imposing laws on foreign jurisdictions. The creation of boarders, via data regulation, in the online world may therefore encourage more aggressive competition not just between businesses, but amongst nations which are participating within the digital economy. Such regulations could result in issues such as surveillance, censorship, and informational inequality. Alternatively, as the GDPR is a blanket regulation with the purpose of harmonizing the diverse laws of each EU nation, a similar effect may gradually arise provided enough nations adopt similar privacy views. This regulatory consistency could simplify the legal landscape, thereby allowing enterprises entry to compete regardless of their size or origin. Subsequently, this increased competition and diversity may positively affect innovation.

5.2 Academic Contribution

While there is a substantial amount of existing literature focused on privacy and innovation, this research study aims to contextualize the current understanding of these topics in light of the relatively new regulation. Although the GDPR's potential global impact is a heavily discussed topic, due to its recency there is not much research examining its effects post-implementation, particularly in regards to non-EU enterprise. Additionally, the identified topics within the discourse, as well as the power interests derived from the data, serve to either support, extend and strengthen, or contrast with current theories. Thus, this research complements existing literature, offering a new perspective.

5.3 Limitations

While the study provides valuable insight into privacy conflicts and discussion in context of business, there are a number of limitations that need to be taken into account when the results are explained. For instance, despite the sample selection for the content analysis being theory-driven, and articles being selected both due to thematic relevance and for the purpose of diversity, a large portion of these came from Western-based sources. However, these sources were mainly international in scope and often concerned non-EU and non-Western nations, thereby mitigating the ramifications associated with this type of limitation. Other common concerns, such as those of validity and reliability also need to be addressed.

5.3.1 Reflexivity

Particularly pertaining to qualitative research as it is highly reliant on the researchers' interpretation, it is important to be aware of the influences that may affect the results. As explained by Jørgensen and Phillips, researchers who are more inclined towards a constructionist perspective understand their research as one version out of many possible interpretations (2002). This reflectivity not only applies to the researcher, but the subjects as well – or authors of the examined data, in the case of this study. An individuals' background, knowledge and experiences will affect their perspective, even in the case of empirical, data-based research (Babbie, 2017). Begin a data subject, and belonging to one of the relevant stakeholder groups within the privacy discourse for example may shape the manner in which the results are interpreted. However, while it is important to recognise these potential biases, such issues do not necessarily diminish the value or significance of the research, provided there is sufficient validity within the study.

5.3.2 Validity

As previously outline in chapter 3, the qualitative validity of this research - comprised of elements such as trustworthiness, authenticity and credibility – has been periodically confirmed throughout the analysis stage in order to ensure consistency and accuracy. Primarily, the most salient covered in chapter 4 were derived from diverse, but converging sources of data, although those that also presented unique perspectives or statements contrary to the theoretical framework were similarly examined and induced. Similarly, constant comparison of topics was done throughout the coding stage in order to improve consistency. If the articles included any factual statements which were not supported by evidence, these were similarly verified, which both served to ensure the reliability of the source, as well as a way of revealing any power interests to be examined within the discourse. Further, the peer debriefing technique was employed as a tool for reflexivity and evaluating researcher bias (Creswell & Creswell, 2018). This included allowing an external source to read sections of the study, discuss and add question, in order to gain an additional perspectives.

5.4 Further Research

As indicated by the findings, the GDPR may result in a variety of long-term effects on enterprises outside the EU in terms of competition and innovation, and as the updated regulation is still relatively new, not enough time has lapsed for these effects to completely surface. Therefore, a longitudinal study regarding further developments, impact and effectiveness would be appropriate. Similarly, public sentiment as well as discourse are constantly changing, hence it may be interesting to observe these changes alongside the development of data legislation. Since the results demonstrated optimism towards the potential opportunities as a result of the regulation, another

potential avenue for further research could be to identify and examine businesses (both within and outside the EU) that have altered their business models based on the values and standards introduced by the GDPR. This may better reveal the direct impact, either positive or negative, of the GDPR – such whether the success of such business has been affected, or whether there has been a change in relationship with their customers. Additionally while there is some focus in existing research on the application of the GDPR within the global market, very few investigate its enforcement systems and strategies. Enforcement is a significant factor when it comes to the effectiveness of regulation – a law will have little effect if no entity exists to invoke it – and is worth exploring. Finally, since governmental entities were revealed to be one of the significant stakeholders in data discourse, the scope of the sampling may be altered in order to specifically examine the topic from the perspective and stance of this group.

Reference List

Abril, P. S., & Lipton, J. D. (2014). The Right To Be Forgotten: Who Decides What the World Forgets. *Ky. LJ*, *103*, 363.

Agahari, W. (2018, December 03). Challenges and Opportunities of the Digital Economy in Indonesia. Retrieved from https://diode.network/2018/11/06/challenges-and-opportunities-of-the-digital-economy-in-indonesia/

Albrecht, J. (2016). How the gdpr will change the world. *European Data Protection Law Review, 2*(3), 287-289. doi:10.21552/EDPL/2016/3/4

Alemanno, A. (2018). Big data for good: Unlocking privately-held data to the benefit of the many. *European Journal of Risk Regulation*, 9(2), 183-191. doi:10.1017/err.2018.34

Aliya, R., & Murphey, H. (2018, July 2). Companies under strain from GDPR requests. Retrieved from https://www-ft-com.eur.idm.oclc.org/content/31d9286a-7bac-11e8-8e67-1e1a0846c475

Almeanno, A. (2018). Big data for good: Unlocking privately-held data to the benefit of the many. *European Journal of Risk Regulation, 9*(2), 183-191. doi:10.1017/err.2018.34

Andrejevic, M. (2014). Big Data, Big Questions| The Big Data Divide.*International Journal Of Communication, 8*, 17. Retrieved from https://ijoc.org/index.php/ijoc/article/view/2161/1163

Arora, P. (2016). Bottom of the data pyramid: Big data and the global south. *International Journal of Communication, 10*, 1681-1699.

Arora, P. (2018). Decolonizing privacy studies. *Television & New Media, 152747641880609*, 152747641880609-152747641880609. doi:10.1177/1527476418806092

Atzori, L., Iera, A., Morabito, G., & Nitti, M. (2012). The social internet of things (siot)–when social networks meet the internet of things: Concept, architecture and network characterization. *Computer networks*, *56*(16), 3594-3608.

Babbie, E. (2017). *The basics of social research* (Seventh ed.). Boston, MA, USA: Cengage Learning.

Bartlett, C., & Ghoshal, S. (2000). Going global: Lessons from late movers. *Harvard Business Review, 78*, 132-145.

Baxter, M. (2018, August 28). How GDPR is shaping global data protection. Retrieved from https://gdpr.report/news/2018/08/24/how-gdpr-is-shaping-global-data-protection/

Beaumont, S. (2018) *The data protection directive versus the GDPR: understanding key changes*. Retrieved from https://gdpr.report/news/2018/03/06/data-protection-directive-versus-gdpr-understanding-key-changes/

Beck, S., & Prügl, R. (2018). Family firm reputation and humanization: Consumers and the trust advantage of family firms under different conditions of brand familiarity. *Family Business Review*, 31(4), 460-482. doi:10.1177/0894486518792692

Beckett, P. (2017). Gdpr compliance: Your tech department's next big opportunity. *Computer Fraud & Security, 2017*(5), 9-13. doi:10.1016/S1361-3723(17)30041-6

Bell, J., & Loane, S. (2010). 'New-wave'global firms: Web 2.0 and SME internationalisation. *Journal of Marketing Management*, *26*(3-4), 213-229.

Bellman, S., Johnson, E. J., Kobrin, S. J., & Lohse, G. L. (2004). International differences in information privacy concerns: A global survey of consumers. *The Information Society*, *20*(5), 313-324.

Bender, D. (2018, June 7). GDPR harmonization: Reality or myth? Retrieved from https://iapp.org/news/a/gdpr-harmonization-reality-or-myth/

Bennett, S. C. (2012). The right to be forgotten: Reconciling EU and US perspectives. *Berkeley J. Int'l L.*, *30*, 161.

Blok, V., & Lemmens, P. (2015). The emerging concept of responsible innovation. Three reasons why it is questionable and calls for a radical transformation of the concept of innovation. In *Responsible Innovation 2* (pp. 19-35). Springer, Cham.

Boyd, D. (2017). Did media literacy backfire?. *Journal of Applied Youth Studies*, *1*(4), 83.

Boyd, D., & Crawford, K. (2012). Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon. *Information, communication & society*, *15*(5), 662-679.

Budish, R. (2017, February 22). Data protection: How are attitudes to disclosure changing? Retrieved from https://www.digitalasiahub.org/2017/02/22/data-protection-how-are-attitudes-to-disclosure-changing/

Bueza, M., & Manuel, W. (2016). Experts fear identity theft, scams due to Comelec leak. Retrieved from https://www.rappler.com/newsbreak/in-depth/127870-comelec-leak-identity-theft-scams-experts

Bukht, R. (2017, August 30). Early regulatory reforms can benefit developing countries in the digital economy. Retrieved from https://diode.network/2017/08/30/early-regulatory-reforms-can-benefit-developing-countries-in-the-digital-economy/

Campbell, C. (n.d.). How China Is Using Big Data to Create a Social Credit Score. Retrieved from http://time.com/collection/davos-2019/5502592/china-social-credit-score/

Cao, J., & Everard, A. (2008). User attitude towards instant messaging: The effect of espoused national cultural values on awareness and privacy. Journal of Global Information Technology Management, 11(2), 30-57.

Chander, A. (2013). How Law Made Silicon Valley. *Emory Law Journal 63.* (2013): 639.

Cho, H., Rivera-Sánchez, M., & Lim, S. S. (2009). A multinational study on online privacy: global concerns and local responses. *New Media & Society*, *11*(3), 395–416.

Ciriani, S. (2015). The economic impact of the european reform of data protection. *Communications & Stratégies / Idate, 97*, 41-58.

Cisco Systems. (2019). Cisco Visual Networking Index: Forecast and Trends, 2017–2022 White Paper. (Whitepaper). Retrieved from https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html#_Toc532256803

Clarip Privacy. (n.d.). GDPR for Small Businesses Under 250 Employees. Retrieved from https://www.clarip.com/blog/gdpr-under-250-employees/

Cohen, J. E. (2014). The surveillance-innovation complex: The irony of the participatory turn. *The Participatory Condition (University of Minnesota Press, 2015, Forthcoming)*.

Connolly, K., Chrisafis, A., Kirchgaessner, S., Haas, B., Hunt, E., & Safi, M. (2016, December 02). Fake news: An insidious trend that's fast becoming a global problem. Retrieved from https://www.theguardian.com/media/2016/dec/02/fake-news-facebook-us-election-around-the-world

Couldry, N., & Mejias, U. (2018). Data colonialism: Rethinking big data's relation to the contemporary subject. *Television & New Media, 152747641879663*, 152747641879663-152747641879663. doi:10.1177/1527476418796632

Creswell, J., & Creswell, J. (2018). *Research design : Qualitative, quantitative, and mixed methods approaches*(Fifth ed.). Thousand Oaks, California: SAGE Publications.

Crichton, D. (2018, May 29). GDPR, China and data sovereignty are ultimately wins for Amazon and Google – TechCrunch. Retrieved from https://techcrunch.com/2018/05/29/gdpr-and-the-cloud-winners/

Crié, D., & Micheaux, A. (2006). From customer data to value: What is lacking in the information chain? *Journal of Database Marketing & Customer Strategy Management*, 13(4), 282–299. http://doi.org/10.1057/palgrave.dbm.3240306

Cunningham, M. (2016). Free Expression, Privacy, and Diminishing Sovereignty in the Information Age: The Internationalization of Censorship. Ark. L. Rev., 69, 71.

Curtiss, T. (2016). Privacy Harmonization and the Developing World: The Impact of the EU's General Data Protection Regulation on Developing Economies. *Wash. JL Tech. & Arts*, *12*, 95.

Degeling, M., Utz, C., Lentzsch, C., Hosseini, H., Schaub, F., & Holz, T. (2018). We Value Your Privacy... Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy. *arXiv preprint arXiv:1808.05096*.

De Hert, P., Papakonstantinou, V., Malgieri, G., Beslay, L., & Sanchez, I. (2018). The right to data portability in the GDPR: Towards user-centric interoperability of digital services. *Computer Law & Security Review*, *34*(2), 193-203.

Digital Literacy. (2018). In McArthur, T., Lam-McArthur, J., & Fontaine, L. (Eds.), *The Oxford Companion to the English Language*. : Oxford University Press,. Retrieved 12 Mar. 2019, from http://www.oxfordreference.com.eur.idm.oclc.org/view/10.1093/acref/9780199661282.001.0001/acref-9780199661282-e-1371.

Dinev, T., Xu, H., Smith, J. and Hart, P. (2012). Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems*, 22(3), pp.295-316.

doi:http://dx.doi.org.eur.idm.oclc.org/10.4018/jgim.2004010102

DOMO. (2018). Data Never Sleeps. (Report No. 6). Retrieved from https://www.domo.com/assets/downloads/18_domo_data-never-sleeps-6+verticals.pdf

Douglas, H. E. (2003). The moral responsibilities of scientists (tensions between autonomy and responsibility). *American Philosophical Quarterly*, *40*(1), 59-68.

Elten, H. (2019, May 26). Europe' data security dilemma: The Huawei debate | GRI. Retrieved from https://globalriskinsights.com/2019/05/europe-data-security-dilemma-the-huawei-debate/

European Commission. (2018a, August 01). *What if my company/organisation fails to comply with the data protection rules?* Retrieved from https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/sanctions/what-if-my-company-organisation-fails-comply-data-protection-rules_en

European Commission. (2018b, August 28). Proposal for an ePrivacy Regulation. Retrieved from https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation

European Commission. (2019). For how long can data be kept and is it necessary to update it? Retrieved from https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/how-long-can-data-be-kept-and-it-necessary-update-it_en

European Union. (2019, March 07). Regulations, Directives and other acts. Retrieved from https://europa.eu/european-union/eu-law/legal-acts_en

Fazlioglu, M. (2013). Forget me not: the clash of the right to be forgotten and freedom of expression on the Internet. *International Data Privacy Law*, *3*(3), 149-157.

Featherly, K. (2016, November 28). ARPANET. Retrieved from https://www.britannica.com/topic/ARPANET

Finn, R., Wright, D., & Friedewald, M. (2013). *Seven types of privacy* (pp. 3-32). doi:10.1007/978-94-007-5170-5_1

Forrest, C. (2018, May 29). GDPR vs. ePrivacy: The 3 differences you need to know. Retrieved from https://www.techrepublic.com/article/gdpr-vs-eprivacy-the-3-differences-you-need-to-know/

Freedom House. (2019). *Democracy in Retreat*. (Report). Retrieved from https://freedomhouse.org/sites/default/files/Feb2019_FH_FITW_2019_Report_ForWeb-compressed.pdf

French, A. M., & Shim, J. P. (2016). The Digital Revolution: Internet of Things, 5G, and Beyond. *CAIS*, *38*, 40.

Fried, C. (1968). Privacy. *The Yale Law Journal, 77*(3), 475-493. doi:10.2307/794941

Gagné, J. (2015). *Hybrid regimes* (Oxford bibliographies. political science). New York: Oxford University Press. (2015). Retrieved May 30, 2019, from INSERT-MISSING-DATABASE-NAME.

Gallagher, G. (2018). SMEs' corporate governance challenge. Accountancy Ireland, 50(4), 36-37. Retrieved from https://search-proquest-com.eur.idm.oclc.org/docview/2123044632?accountid=13598

Ganesh, M.I.; Deutch, J. and Schulte,J. (2016) *Privacy, anonymity, visibility: dilemmas in tech use by marginalize communities*, Brighton: IDS

Goldfarb, A., & Tucker, C. (2012). Privacy and innovation. *Innovation policy and the economy*, *12*(1), 65-90.

Groves, C. (2006). Technological futures and non-reciprocal responsibility. *The international journal of the humanities*, *4*(2), 57-61.

Hargittai, E., & Hinnant, A. (2008). Digital inequality: Differences in young adults' use of the Internet. *Communication research*, *35*(5), 602-621.

Hemphill, T. (2002). Electronic commerce and consumer privacy: Establishing online trust in the u.s. digital economy. *Business and Society Review, 107*(2), 221-239. doi:10.1111/1467-8594.00134

Henkin, L. (1974). Privacy and autonomy. *Columbia Law Review, 74*(8), 1410-1410. doi:10.2307/1121541

Hill, R. (2019, January 25). French data watchdog dishes out largest GDPR fine yet: Google ordered to hand over €50m. Retrieved from https://www.theregister.co.uk/2019/01/21/google_50m_cnil_gdpr/

Hofstede, G., & Triandis, H. (1993). Cultures and organizations: Software of the mind. *Administrative Science Quarterly, 38*(1), 132-133.

Huang, F. (2018, December 31). The Rise and Fall of China's Cycling Empires. Retrieved from https://foreignpolicy.com/2018/12/31/a-billion-bicyclists-can-be-wrong-china-business-bikeshare/

IDC (International Data Corporation). (2019, January 3). IDC Forecasts Worldwide Spending on the Internet of Things to Reach $745 Billion in 2019, Led by the Manufacturing, Consumer, Transportation, and Utilities Sectors. Retrieved from: https://www.idc.com/getdoc.jsp?containerId=prUS44596319

International Business Machines Corporation [IBM]. (2018, May). The end of the beginning: Unleashing the transformational power of GDPR. *Executive Report*. Retrieved from https://www.ibm.com/downloads/cas/JEMXN6LV

Jeffrey Toobin. (2014, September 22). The Solace of Oblivion. *The New Yorker.* Retrieved from: https://www.newyorker.com/magazine/2014/09/29/solace-oblivion

Jørgensen, M. & Phillips, L. (2002). *Discourse Analysis as Theory and Method* (1st ed.). Thousand Oaks, CA: Sage.

Kalathil, S., & Boas, T. (2001). The internet and state control in authoritarian regimes: China, cuba and the counterrevolution. *First Monday, 6*(8). doi:10.5210/fm.v6i8.876

Kelly, B. (2018, October 31). Blasphemy laws and punishments from around the world. Retrieved from https://www.independent.co.uk/news/world/europe/ireland-blasphemy-referendum-irish-religion-illegal-remove-ban-countries-world-laws-a8597391.html

Kemp, D. (2019, February 14). The GDPR paradox: How data regulation creates revenue streams. Retrieved from https://www.techradar.com/news/the-gdpr-paradox-how-data-regulation-creates-revenue-streams

Kendall, C. (2009, March 29). China's global cyber-espionage network GhostNet penetrates 103 countries. Retrieved from https://www.telegraph.co.uk/news/worldnews/asia/china/5071124/Chinas-global-cyber-espionage-network-GhostNet-penetrates-103-countries.html

Kerr, J. A. (2018). *The Russian Model of Internet Control and Its Significance* (No. LLNL-TR-764577). Lawrence Livermore National Lab.(LLNL), Livermore, CA (United States).

Kleist, V. (2004). A transaction cost model of electronic trust : Transactional return, incentives for network security and optimal risk in the digital economy. *Electronic Commerce Research, 4*(1), 41-57.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers & Security, 64, 122-134. doi:10.1016/j.cose.2015.07.002

Kosinski, M., Stillwell, D., & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences*, *110*(15), 5802-5805.

Kuner, C., Cate, F., Millard, C., & Svantesson, D. (2012). The challenge of 'big data' for data protection. *International Data Privacy Law, 2*(2), 47-49. doi:10.1093/idpl/ips003

Larson III, R. G. (2013). Forgetting the First Amendment: How obscurity-based privacy and a right to be forgotten are incompatible with free speech. *Communication Law and Policy*, *18*(1), 91-120.

LaValle, S., Lesser, E., Shockley, R., Hopkins, M. S., & Kruschwitz, N. (2011). Big data, analytics and the path from insights to value. *MIT sloan management review*, *52*(2), 21.

Levin, B. (2018, September 26). Quantcast reports more than 90% of visitors to EU domains grant GDPR consent. Retrieved April 12, 2019, from https://martechtoday.com/quantcast-reports-more-than-90-of-visitors-to-eu-domains-grant-gdpr-consent-219462

Li, B. (2018, January). Personal information security specification. Retrieved from https://www.nortonrosefulbright.com/en/knowledge/publications/f959f04d/personal-information-security-specification

Li, H., Yu, L., & He, W. (2019). The Impact of GDPR on Global Technology Development, *Journal of Global Information Technology Management*, 22:1, 1-6, DOI: 10.1080/1097198X.2019.1569186

Liu, C., Marchewka, J. T., & Ku, C. (2004). American and taiwanese perceptions concerning privacy, trust, and behavioral intentions in electronic commerce.*Journal of Global Information Management, 12*(1), 18-40.

Lovejoy, B. (2019, May 28). GDPR fines total €56M in first year as Facebook under scrutiny. Retrieved from https://9to5mac.com/2019/05/28/gdpr-fines/

Lowry, B., Cao, J., & Everard, A. (2011) Privacy Concerns Versus Desire for Interpersonal Awareness in Driving the Use of Self-Disclosure Technologies: The Case of Instant Messaging in Two Cultures, Journal of Management Information Systems, 27:4, 163-200, DOI: 10.2753/MIS0742-1222270406

Lührmann, A., Dahlum S., Lindberg, S. I., Maxwell, L., Mechkova, V., Olin, M., Pillai, S., Petrarca, C. S., Sigman, R., Stepanova, N. (2018). V-Dem Annual Democracy Report 2018. Sweden: V-Dem Institute. Retrieved from: https://www.v-dem.net/media/filer_public/3f/19/3f19efc9-e25f-4356-b159-b5c0ec894115/v-dem_democracy_report_2018.pdf

Macey, J., & Hamari, J. (2019). eSports, skins and loot boxes: Participants, practices and problematic behaviour associated with emergent forms of gambling. *new media & society*, *21*(1), 20-41.

Mansfield-Devine, S. (2016). Securing small and medium-size businesses. Network Security, 2016(7), 14-20. doi:10.1016/S1353-4858(16)30070-8

Mantelero, A. (2013). The eu proposal for a general data protection regulation and the roots of the 'right to be forgotten'. *Computer Law & Security Review: The International Journal of Technology Law and Practice,29*(3), 229-235. doi:10.1016/j.clsr.2013.03.010

Mayer-Schönberger, V., & Cukier, K. (2013). *Big data. A revolution that will transform how we live, work, and think*. New York: Houghton Mifflin Harcourt.

McAfee, A., & Brynjolfsson, E. (2012). Big data: The management revolution. *Harvard Business Review, 90*(10), 59–68.

Milberg, S. J., Burke, S. J., Smith, H. J., & Kallman, E. A. (1995). Values, personal information privacy, and regulatory approaches. *Association for Computing Machinery.Communications of the ACM, 38*(12), 65. Retrieved from https://search-proquest-com.eur.idm.oclc.org/docview/237033462?accountid=13598

Miltgen, C., & Peyrat-Guillard, D. (2014). Cultural and generational influences on privacy concerns: A qualitative study in seven european countries. *European Journal of Information Systems, 23*(2), 103-125. doi:10.1057/ejis.2013.17

Monteiro, R. L. (2018, August 15). The new Brazilian General Data Protection Law - a detailed analysis. Retrieved from https://iapp.org/news/a/the-new-brazilian-general-data-protection-law-a-detailed-analysis/

Moore, A. (2008). Defining privacy. *Journal of Social Philosophy, 39*(3), 411-428. doi:10.1111/j.1467-9833.2008.00433.x

Norberg, P., & Horne, D. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs, 41*(1), 100-126.

Nuttley, M. (2016, November 1). Privacy And Innovation Are Not Mutually Exclusive. Retrieved from https://www.cmo.com/features/articles/2016/10/31/privacy-and-innovation-are-not-mutually-exclusive.html#gs.clp7hb

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing, 19*(1), 27-41. doi:http://dx.doi.org.eur.idm.oclc.org/10.1509/jppm.19.1.27.16941

Politou, E., Michota, A., Alepis, E., Pocs, M., & Patsakis, C. (2018). Backups and the right to be forgotten in the gdpr: An uneasy relationship. *Computer Law & Security Review, 34*(6), 1247-1257. doi:10.1016/j.clsr.2018.08.006

Porter, J. (2019, January 21). Google fined €50 million for GDPR violation in France. Retrieved from https://www.theverge.com/2019/1/21/18191591/google-gdpr-fine-50-million-euros-data-consent-cnil

Porter, J. (2019, January 27). GDPR makes it easier to get your data, but that doesn't mean you'll understand it. Retrieved from https://www.theverge.com/2019/1/27/18195630/gdpr-right-of-access-data-download-facebook-google-amazon-apple

PricewaterhouseCoopers [PWC]. (2018, January). *Technology's Role in Data Protection – The Missing Link in GDPR Transformation*. (Report). Retrieved from https://www.pwc.com/gx/en/issues/regulation/technologys-role-in-data-protection-the-missing-link-in-gdpr-transformation.pdf

Privacy International (2013, December). *A New Dawn: Privacy in Asia*. (Report). Retrieved from https://privacyinternational.org/sites/default/files/2017-12/A%20New%20Dawn_Privacy%20in%20Asia.pdf

Privacy International. (2018, April 9*) Data Is Power: Profiling and Automated Decision-Making in GDPR.* (Report). Retrieved from https://privacyinternational.org/report/1718/data-power-profiling-and-automated-decision-making-gdpr

Privacy International. (2019a, March 13). Tech giants do not face enough competition, new report says. Retrieved from https://privacyinternational.org/news/2763/tech-giants-do-not-face-enough-competition-new-report-says

Privacy International. (2019b, April 15) New faith in privacy regulation? We need proof of conversion. (Blog) Retrieved from https://privacyinternational.org/blog/2815/new-faith-privacy-regulation-we-need-proof-conversion

Puschmann, C., & Burgess, J. (2014). Big Data, Big Questions| Metaphors of Big Data. *International Journal Of Communication, 8*, 20. Retrieved from https://ijoc.org/index.php/ijoc/article/view/2169

R & G Technologies. (N.d.). Data Sovereignty. Retrieved from: https://rgtechnologies.com.au/resources/data-sovereignty/

Ranking countries by their blasphemy laws. (2017, August 13). Retrieved from https://www.economist.com/erasmus/2017/08/13/ranking-countries-by-their-blasphemy-laws

Reiman, J. (1976). Privacy, Intimacy, and Personhood. *Philosophy & Public Affairs, 6*(1), 26-44. Retrieved from http://www.jstor.org.eur.idm.oclc.org/stable/2265060

Robertson, J., & Riley, M. (2018, October 4). The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies. Retrieved from https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltr ate-america-s-top-companies

Robinson, L., Cotten, S., Ono, H., Quan-Haase, A., Mesch,G., Chen, W., Schulz, J., Hale, M., T., & Stern, J., M., (2015) Digital inequalities and why they matter. *Information, Communication & Society*,18:5, 569-582, DOI: 10.1080/1369118X.2015.1012532

Rogers,E., M. (1995). Diffusion of innovations. *New York*, *12*.

Rousseau, D., & Sitkin, S. (1998). Not so different after all: A cross-discipline view of trust. *Academy of Management Review*.

Rosen, J. (2011). The right to be forgotten. *Stan. L. Rev. Online*, *64*, 88.

Rubinstein, I. (2013). Big data: The end of privacy or a new beginning? *International Data Privacy Law, 3*(2), 74-87. doi:10.1093/idpl/ips036

Sacks, S. (2018, March). China's Emerging Data Privacy System and GDPR. Retrieved from https://www.csis.org/analysis/chinas-emerging-data-privacy-system-and-gdpr

Safari, B. (2017). Intangible privacy rights: How europe's gdpr will set a new global standard for personal data protection. *Seton Hall Law Review, 47*(3), 809-848.

Santanen, E. (2019). The value of protecting privacy. *Business Horizons, 62*(1).

SeeUnity. (2018). *The main differences between the DPD and the GDPR and how to address those moving forward* [White paper]. Retrieved from https://britishlegalitforum.com/wp-content/uploads/2017/02/GDPR-Whitepaper-British-Legal-Technology-Forum-2017-Sponsor.pdf

Shoor, E. A. (2014). Narrowing the right to be forgotten: why the European Union needs to amend the proposed data protection regulation. *Brook. J. Int'l L.*, *39*, 487.

Silber, T. (2019, February 28). GDPR Gives European Tech Companies A Major Advantage, Two EU-Based CMOs Say. Retrieved from

https://www.forbes.com/sites/tonysilber/2019/02/28/gdpr-gives-european-tech-companies-a-major-advantage-two-eu-based-cmos-say/#4fe7e7d1713f

Silverman, C. (2011, June 17). The Backfire Effect: More on the press's inability to debunk bad information. Retrieved from https://archives.cjr.org/behind_the_news/the_backfire_effect.php

Solove, D.J. (2008). Understanding Privacy. Cambridge, MA: Harvard University Press.

Springman, J. (2018, May 15). Why complying with GDPR is not enough. Retrieved from https://www.ctrl-shift.co.uk/news/2018/05/15/why-complying-with-gdpr-is-not-enough/

Stahl, B. C. (2013). Responsible research and innovation: The role of privacy in an emerging framework. *Science and Public Policy*, *40*(6), 708-716.

Stilgoe, J., Owen, R., & Macnaghten, P. (2013). Developing a framework for responsible innovation. Research Policy, 42(9), 1568-1580.

Sumner, A. (2016). *Global poverty : Deprivation, distribution and development since the cold war*(First ed.) [First edition.]. Oxford: Oxford University Press. (2016). Retrieved June 4, 2019, from INSERT-MISSING-DATABASE-NAME.

Tanash, R. S., Chen, Z., Thakur, T., Wallach, D. S., & Subramanian, D. (2015, October). Known unknowns: An analysis of Twitter censorship in Turkey. In *Proceedings of the 14th ACM Workshop on Privacy in the Electronic Society* (pp. 11-20). ACM.

Taylor, A. (2018, March 22). The Bike-Share Oversupply in China: Huge Piles of Abandoned and Broken Bicycles. Retrieved from https://www.theatlantic.com/photo/2018/03/bike-share-oversupply-in-china-huge-piles-of-abandoned-and-broken-bicycles/556268/

Taylor, C., & Fosler, G. D. (1994). The necessity of being global. *Across the Board*, *31*(2), 40-43.

Teads. (2018, November 14). GDPR: Only 5% of European users refuse cookies used for personalised advertising. Retrieved from https://www.teads.com/gdpr-only-5-of-european-users-refuse-cookies-used-for-personalised-advertising/

Toobin, J. (2014, September 22). The Solace of Oblivion. Retrieved from https://www.newyorker.com/magazine/2014/09/29/solace-oblivion

Twitter. (2018). *Removal requests*. Retrieved from: https://transparency.twitter.com/en/removal-requests.html

Twitter. (2019). Information Requests. (Report). Retrieved from https://transparency.twitter.com/en/information-requests.html

Urban, T., Tatang, D., Degeling, M., Holz, T., & Pohlmann, N. (2018). The Unwanted Sharing Economy: An Analysis of Cookie Syncing and User Transparency under GDPR. *arXiv preprint arXiv:1811.08660*.

USForex. 2016. Global Expansion Meets Domestic and International Challenges. Retrieved from https://www.ofx.com/-/media/files/pdfs/temp/confidence_indicator_report_usforex_final.pdf/

Van Deursen, A., & Van Dijk, J. (2011). Internet skills and the digital divide. *New Media & Society, 13*(6), 893-911.

Van Dijck, J. (2014). Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & Society*, *12*(2), 197-208.

Von Schomberg, R. (2013). Responsible innovation. In *A vision of responsible research and innovation* (pp. 51-74). John Wiley & Sons, Ltd : Chichester, UK. doi:10.1002/9781118551424.ch3

Wang, M. (2018, June 01). GDPR, EU's Commitment to Tech Giants' Monopoly. Retrieved from https://medium.com/@miccowang/gdpr-eus-commitment-to-tech-giants-monopoly-42ca626bdd0f

Weber, R. H. (2011). The right to be forgotten: More than a Pandora's box. *J. Intell. Prop. Info. Tech. & Elec. Com. L.*, *2*, 120. The right to be forgotten seen in the us as a limitation of free speech

Westin, A. (1967). *Privacy and freedom*. New York: Atheneum.

Whitman, J. (2004). The Two Western Cultures of Privacy: Dignity versus Liberty. *The Yale Law Journal, 113*(6), 1151-1221. doi:10.2307/4135723

Whittaker, Z. (2019, February 01). Indian state government leaks thousands of Aadhaar numbers – TechCrunch. Retrieved from https://techcrunch.com/2019/01/31/aadhaar-data-leak/

Wilkinson, G. (2018, July 1). General Data Protection Regulation: No silver bullet for small and medium-sized enterprises. Journal of Payments Strategy & Systems, Volume 12 (Number 2). Retrieved from https://www.ingentaconnect.com/content/hsp/jpss/2018/00000012/00000002/art00006

Williams, R. (n.d.). Data Volumes. Retrieved from https://www.eecis.udel.edu/~amer/Table-Kilo-Mega-Giga---YottaBytes.html

Wong, M. (2017, September 29). Pizza over privacy? Stanford economist examines a paradox of the digital age | Stanford News. Retrieved September 30, 2018, from https://news.stanford.edu/2017/08/03/pizza-privacy-stanford-economist-examines-paradox-digital-age/

Xiaolong, J., Wah, B., W., Cheng, X., Wang, Y. (2015). Significance and challenges of big data research. *Big Data Research* 2.2 (2015): 59-64.

Yu, E. (2019, January 14). Employees sacked, CEO fined in SingHealth security breach. Retrieved from https://www.zdnet.com/article/employees-sacked-ceo-fined-in-singhealth-security-breach/

Zarsky, T. (2017). The privacy-innovation conundrum. *Intellectual Property and Innovation, Vol. 2, Pages 804-857.*

Zendle, D., & Cairns, P. (2018). Video game loot boxes are linked to problem gambling: Results of a large-scale survey. *PloS one*, *13*(11), e0206767.

Appendix A

List of Data used in Analysis

No.	Key	
	Type 1: Academic Articles	
1	Big Data for Good: Unlocking Privately-Held Data to the Benefit of the Many	Alemanno, A. (2018). Big data for good: Unlocking privately-held data to the benefit of the many. European Journal of Risk Regulation, 9(2), 183-191. doi:10.1017/err.2018.34
2	We Value Your Privacy ... Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy	Degeling, M., Utz, C., Lentzsch, C., Hosseini, H., Schaub, F., & Holz, T. (2018). We Value Your Privacy... Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy. *arXiv preprint arXiv:1808.05096*.
3	The Unwanted Sharing Economy: An Analysis of Cookie Syncing and User Transparency under GDPR	Urban, T., Tatang, D., Degeling, M., Holz, T., & Pohlmann, N. (2018). The Unwanted Sharing Economy: An Analysis of Cookie Syncing and User Transparency under GDPR. arXiv preprint arXiv:1811.08660.
	Type 2: Blogs and Articles	
4	The Solace of Oblivion	Toobin, J. (2014, September 22). The Solace of Oblivion. Retrieved from https://www.newyorker.com/magazine/2014/09/29/solace-oblivion
5	Eurrope Finally Agrees Touch New Data Protection Rules	Lomas, N. (2015, December 16). Europe Finally Agrees Tough New Data Protection Rules. Retrieved from https://techcrunch.com/2015/12/16/gdpr-agreed/
6	EU 'right to be forgotten' ruling paves way for cencorship	Solon, O. (2017, October 04). EU 'right to be forgotten' ruling paves way for censorship. Retrieved from https://www.wired.co.uk/article/right-to-be-forgotten-blog
7	Why complying with GDPR is not enough	Springman, J. (2018, May 15). Why complying with GDPR is not enough. Retrieved from https://www.ctrl-shift.co.uk/news/2018/05/15/why-complying-with-gdpr-is-not-enough/
8	Privacy And Innovation Are Not Mutually Exclusive	Nuttley, M. (2016, November 1). Privacy And Innovation Are Not Mutually Exclusive. Retrieved from https://www.cmo.com/features/articles/2016/10/31/privacy-and-innovation-are-not-mutually-exclusive.html#gs.clp7hb
9	GDPR, EU's Commitment to Tech Giants' Monopoly	Wang, M. (2018, June 01). GDPR, EU's Commitment to Tech Giants' Monopoly. Retrieved from https://medium.com/@miccowang/gdpr-eus-commitment-to-tech-giants-monopoly-42ca626bdd0f

10	GDPR, China and data sovereignty are ultimately wins for Amazon and Google	Crichton, D. (2018, May 29). GDPR, China and data sovereignty are ultimately wins for Amazon and Google – TechCrunch. Retrieved from https://techcrunch.com/2018/05/29/gdpr-and-the-cloud-winners/
11	GDPR Gives European Tech Companies A Major Advantage, Two EU-Based CMOs Say	Silber, T. (2019, February 28). GDPR Gives European Tech Companies A Major Advantage, Two EU-Based CMOs Say. Retrieved from https://www.forbes.com/sites/tonysilber/2019/02/28/gdpr-gives-european-tech-companies-a-major-advantage-two-eu-based-cmos-say/#4fe7e7d1713f
12	The GDPR paradox: how data regulation creates revenue streams	Kemp, D. (2019, February 14). The GDPR paradox: How data regulation creates revenue streams. Retrieved from https://www.techradar.com/news/the-gdpr-paradox-how-data-regulation-creates-revenue-streams
13	New faith in privacy regulation? We need proof of conversion	Privacy International. (2019b, April 15) New faith in privacy regulation? We need proof of conversion. (Blog) Retrieved from https://privacyinternational.org/blog/2815/new-faith-privacy-regulation-we-need-proof-conversion
14	Tech giants do not face enough competition, new report says	Privacy International. (2019a, March 13). Tech giants do not face enough competition, new report says. Retrieved from https://privacyinternational.org/news/2763/tech-giants-do-not-face-enough-competition-new-report-says
15	Data protection: How are attitudes to disclosure changing?	Budish, R. (2017, February 22). Data protection: How are attitudes to disclosure changing? Retrieved from https://www.digitalasiahub.org/2017/02/22/data-protection-how-are-attitudes-to-disclosure-changing/
16	Early regulatory reforms can benefit developing countries in the digital economy	Bukht, R. (2017, August 30). Early regulatory reforms can benefit developing countries in the digital economy. Retrieved from https://diode.network/2017/08/30/early-regulatory-reforms-can-benefit-developing-countries-in-the-digital-economy/
17	Challenges and Opportunities of the Digital Economy in Indonesia	Agahari, W. (2018, December 03). Challenges and Opportunities of the Digital Economy in Indonesia. Retrieved from https://diode.network/2018/11/06/challenges-and-opportunities-of-the-digital-economy-in-indonesia/
18	From Silicon Valley to Silicon Savannah? Tech Hubs in the Global South	Zheng, Y. & Cisneros, A., J. (2018, December 17). From Silicon Valley to Silicon Savannah? Tech Hubs in the Global South. Retrieved from https://diode.network/2018/12/17/from-silicon-valley-to-silicon-savannah-tech-hubs-in-the-global-south/
19	GDPR makes it easier to get your data, but that doesn't mean you'll understand it.	

		Porter, J. (2019, January 27). GDPR makes it easier to get your data, but that doesn't mean you'll understand it. Retrieved from https://www.theverge.com/2019/1/27/18195630/gdpr-right-of-access-data-download-facebook-google-amazon-apple
	Type 3: Reports	
20	Technology's role in data protection - the missing link in GDPR transformation	PricewaterhouseCoopers [PWC]. (2018, January). *Technology's Role in Data Protection – The Missing Link in GDPR Transformation*. (Report). Retrieved from https://www.pwc.com/gx/en/issues/regulation/technologys-role-in-data-protection-the-missing-link-in-gdpr-transformation.pdf
21	The end of the beginning - unleashing the transformative power of GDPR	International Business Machines Corporation [IBM]. (2018, May). The end of the beginning: Unleashing the transformational power of GDPR. *Executive Report*. Retrieved from https://www.ibm.com/downloads/cas/JEMXN6LV
22	Data Is Power: Profiling and Automated Decision-Making in GDPR	Privacy International. (2018, April 9) Data Is Power: Profiling and Automated Decision-Making in GDPR. (Report). Retrieved from https://privacyinternational.org/report/1718/data-power-profiling-and-automated-decision-making-gdpr