Public versus private mechanisms for global data protection enforcement: A comparative analysis

by Edona Potera

LLM Final Thesis
SUPERVISOR: Tommaso Soave
Central European University - Private University

20 June 2022

Acknowledgements

To my parents,

Nazmije & Rexhep Potera

Table of Contents

Public versus private mechanisms for global data protection enforcement: A comparative analysis

Introduction

Privacy is a contested concept. It can be described as a right that relates to individuals and their potential ability to determine what particular aspects of themselves to not communicate to others. Privacy has been linked to the concepts of personhood and over decades, the privacy concept has been much discussed, in multiple contexts (Holvast,2009).

The original exploration of privacy as a legal right was made by Warren and Brandeis (1890) who defined privacy as a protection of an individual and the right "to be let alone." (Cooley, 1888) In the contemporary digital world of Big Data, this right "to be let alone" is more difficult to conceptualize, but in general it reflects the right to privacy surrounding digital information that pertains to personal attributes of individuals (Rominsky and Nonisky,2020).

"Moreover, recent developments in social contract theory maintain that a proper understanding of privacy requires an acknowledgement of dialogues around not only rights but also norms". (Martin, 2016). Norms here refer to important contextual factors, outside legal environments, and broader political and social discourses (Martin K., 2016). It is norms, in concert with rights, that form the basis of both explicit and implicit social contracts which govern the practice and obligation of sharing information (Martin K. 2016).

However, regardless of the contextual nature, as the relationship between privacy and the use of data has grown stronger, so has the awareness that this form of privacy should be protected. Hence the right to data protection, as a subset of the privacy right, has recently been a constant element of various jurisdictions, which (jurisdictions) intend to impede actions that endanger the individuals' personal data safeguard (Gstrein and Beauieu,2022).

In fact, with the new legal and ethical risks that the production and consumption of Big Data generates, (Rouvroy, 2016)high-profile incidents involving Big Data, such as Cambridge Analytica, where large data sets were used to identify and target voters during both the US presidential election and the UK's Brexit decision (Scott,,2018,) and other broad challenges posed by the ever-expanding era of giant corporations' personal data footprints, personal data protection is truly of great importance to public regulatory regimes.

Against this backdrop, many scholars have formulated various statutes and public regulations that a number of countries around the world have enacted to ensure some degree of data protection to their populace. By contrast, few have explored the private mechanisms for data protection enforcement adopted by multinational tech companies themselves, which are often seen as lacking in rigor and normative force. Therefore, this thesis seeks to fill this gap by comparing public and private data protection mechanisms and evaluating their impact on the future of data protection governance.

From the perspective of the public regulatory enforcement, the design of data protection framework is heavily influenced by the jurisdictions' approach to privacy, first and foremost.

For instance, the European Union has historically included the right to privacy among fundamental human rights, beginning with the European Union Charter of 2009, which defines

privacy and data protection as fundamental freedoms. In this regard, the EU's regulatory response to Big Data has been gradually strengthened, with the European Commission's General Data Protection Regulation (GDPR) emerging to address rising concerns about Big Data collection. This new 'gold standard'(European Commission, 2018) of data protection regulation imposes costly modifications to the activities of all organizations working with data pertaining to European residents, as well as the possibility of severe fines and penalties for noncompliance.

In this regard, the GDPR has been also acclaimed in the popular press in the United States, (Howell, 2018) some have urged the U.S. entities to voluntarily embrace its provisions (Satariano, 2018), or others even called on imposing some of the GDPR's restrictions (Markey, 2018). Nevertheless, many American policymakers have observed that the GDPR is not suited for the U.S., among other factors, mostly due to the fact that regulatory approaches to privacy are driven by cultural norms and differ significantly among countries.(Hofstede, 2018)

In this context, the cultural differences and exigencies highlight the disparities in approaches to data protection and privacy between the United States and the EU (Jeremy Hainsworth, 1994). For instance, Hofstede's study on the cultural aspects of citizens in the United States and Germany and their implications for data protection policy highlights that Americans place a high value on individualism, engaging with strangers, and seeking knowledge from others, but Germans place a high value on uncertainty avoidance and may be more careful with information sharing (Hofstede,2018).Considering that the GDPR's primary architects are German and Austrian may indicate a cultural intention to either reduce or prevent the uncertainty in the data-driven economy, whereas the Americans may argue that the advantages of sharing information exceed the concerns of future inaccurate information. (Layton & Mclendon,2019).

Despite the lack of a comprehensive federal data protection law in the United States, privacy and data protection have long been included in common law torts, criminal laws, evidentiary privileges, federal statutes, and state laws (Daniel J.Solove, 2006). Additionally, the U.S. is renowned for the longstanding judicial scrutiny and case law, in contrast to the EU whose data protection regulations are relatively new.

Moreover, considering that the American concept of privacy is based in large part on freedom from government interference and as a counterweight to the expansion of the administrative state. (Daniel J.Solove, 2006), the thesis established that while the European mindset indeed reflect the privacy and data protection's foundational value in ensuring human dignity, and self-determination, the U.S. does not approach the right to privacy as a fundamental human right, but rather considers it as a commercial asset, that of a business-oriented approach.

Thereby, this business-oriented approach reflects the core motivation of the U.S. multinational technological corporations' private mechanism on setting new privacy policies.

"From the perspective of the private enforcement of data protection, the data-driven economy has given rise to 'data-opolies'— i.e. the situation where companies that dominate a critical platform, which like a coral reef attracts users, merchants, advertising, software developers, app developers, and accessory makers to its ecosystem" (Stucke, 2016). For instance, Amazon has the largest online merchant platform; Apple and Google each dominate a prominent mobile phone operating system (as well as essential apps on that platform); and Facebook controls the

leading social networking platform (Stucke, 2016) The velocity, volume, variety, and the value of the personal data obtained and exploited by these corporations enables them to gain substantial market influence .

Due to the market influence that companies gain through data processing, this thesis views Big Data as an 'industry' or social, political, and economic system, rather than simply a set of technological practices (Martin 2015).

Therefore, the significant market power of the leading corporations, combined with the US business-oriented privacy mindset, where much privacy regulation is partially based on a self-regulatory approach, might go two ways. First, this can either lead in the Internet being a deregulated territory, where tech and social media businesses have long practiced an anything-goes philosophy, or in understanding the influence of their behavior on the entire society, making their responsibility to protect consumers' right to data protection a priority and thus embracing it beyond the law's requirements.

Regarding this, taking a step back to examine Facebook's history of privacy issues provides an important perspective on how deregulatory online platforms might be and to what serious extent they can attain. For instance, the 2018 Facebook-Cambridge Analytica data privacy scandal, in which Cambridge Analytica illegally collected data from tens of millions of Facebook users and exploited it to generate voter profiles (Scott, 2018,), is just one of the enormous blows to people's faith and confidence in the social networking sites and digital platforms in general.

On the other hand, the Apple 2021 software update(Apple, iOS 14 update), has raised the ethical bar for maintaining and supporting personal data privacy to a higher standard that goes beyond the GDPR's requirements.

In particular, the App Tracking Transparency pop-up, that asks iPhone and iPad users if they want the app to "monitor their behavior across other firms' apps and websites" (Apple, 2021), has left multiple repercussions. First, other tech actors must decide whether to follow the current Apple's 'privacy trend' or continue to be part of Big Tech's snooping and data collecting. Second, the iOS 14.5 Update has significantly impacted the various media channels, social media platforms, and other Google-related ad campaigns in terms of reducing their retargeting audience, which, simply put, means billions of dollars lost.

The two illustrations drawn above, the personal data exploitation case involving millions of individuals and the current Apple's mammoth push for a two-tier privacy system, provide an important understanding of how profound the market power impact of the major tech world is demonstrated to be in the global data policy enforcement.

Finally, this thesis aims at comparing the features and models of public regulatory regime on data protection with self-regulatory regime. In conducting such a review, I will discuss the merits and drawbacks of such regulatory regimes. In particular, the thesis' comparative lens will center around the rights of data subjects concerning data protection.

The following is the order in which this thesis will be structured.

The first chapter deals with introducing the major data protection regime in the European Union, namely GDPR, and discusses whether it is truly a global leader in data protection, (e.g. the regulation of personal information), influencing legislative and corporate policy the world

over (Bradford, 2020). The first chapter evaluates the structure and design of GDPR and discusses its strengths and weaknesses from the perspective of welfare of data subjects and the global governance of data protection.

In the second chapter, the thesis will introduce the private data protection mechanism through the lens of multinational company privacy notices and private awareness tools designed to empower its users through stronger privacy standard practices. This chapter reviews the strengths and weaknesses of private mechanisms.

These two chapters will provide a background to launch into a discussion of how these regimes compare in terms of rights enforcement. Based on such a comparative analysis, the thesis concludes that none of these mechanisms is comprehensive, and that both mechanisms must be viewed as complementary when devising data protection strategies.

Research questions:

The thesis is driven by two central research questions.

The first being: What impact do multinational technology corporations' private mechanisms for setting new privacy standards have on global data policy enforcement?

The second question being: how do those private mechanisms compare to public regulatory mechanisms, such as the General Data Protection Regulation?

Methodology

On the whole, this thesis will compare the existing and prospective mechanisms for data privacy enforcement privately adopted by big tech corporations' against the public data protection regulations adopted in a number of countries, most notably the EU.

First, defining the distinction between GDPR and self-regulatory approaches to privacy and personal data protection is contingent upon the cultural norms. Such an understanding is essential for the continuation of the thesis analysis, as it allows us all to continue uncovering the background and rationale of the current and upcoming private mechanisms as well as the public regulatory framework.

Secondly, this thesis' core conclusion is evaluated with respect to the comparison between large data corporations' private mechanisms and data protection public regulatory framework. In particular, concerning the private mechanism, this review will include a comparison that examines big corporations' privacy policies, their potential capacity to address the latest privacy concerns, and private enforcement remedies.

Likewise, as far as the evaluation of data protection public regulatory regime is concerned, the chapter will include an examination of public regulations enforcement instruments and supervisory authorities.

Thirdly, developing such a framework leads the discussion towards an evaluation of the strengths and weaknesses of such regimes.

To this end, the comparative methodological approach is best suited to this thesis. It is due to the fact that adopting a comparative angle helps to contrast and bring forth the distinction features of data protection regimes.

The thesis research methodology, in particular, presents a comparative research methodology that analyzes the coexistence of public and private data protection regulatory regimes, the differences in their instruments and outcomes, and then brings them together to evaluate the merits and drawbacks of the overall data protection governance.

This research will mainly be based upon the examination and scrutiny of the following legal resources: Firstly, the thesis utilizes primary sources, including legislative instruments such as the text of GDPR. Secondly, the thesis narrative will be informed by secondary sources such as EU Guidelines of Working Parties, and academic commentary of GDPR and private mechanisms. The academic commentary consists of scholarly articles on both data protection regimes, as well as handbooks and textbooks on the interpretation and application of GDPR.

Significance of the thesis

In the contemporary times, where digital technologies have greatly magnified our life possibilities, they have also created a host of challenges, which pertain to our human rights. In particular, where digital technology has facilitated and eased the transfer of data, such data generation has also given rise to modern day problems such as data protection breaches, and infringement of rights to privacy. In the wake of such technological interfaces becoming widespread, and the ensuing challenges that arise, the legal mechanisms have also evolved to come up to terms. However, the elusive question is whether such legal regulatory regimes have actually risen to the challenge. Some of the most pertinent and topic of such laws include privacy and data protection laws, with GDPR being one of the most promising and prominent of such legal developments.

It is in this context that we can analyze that more often than not such privacy laws are a collection of highly authoritative legislation, and highest degree of constitutional norms, regulatory measures, and court decisions. Nonetheless, despite this well-developed and elegant pedigree, such laws have never stood as challenged as they are now —due to the highly digitizing world. Such laws arguably fail to provide and safeguard the data protection rights of the data subjects. For instance, in the context of GDPR, its legislative provisions have been criticized as bureaucratic, top-down, and lacking adequate participation by citizens (Bamberger and Mulligan, 2015). Similarly, the GDPR's response to Big Data has sparked a heated discussion over its incompatibility with the data environment. Furthermore, while we are witnessing an exponential increase in the number of data protection breaches lately, the emergence of GDPR, at least seemingly, has not played a meaningful role in bringing them to an end.

In the wake of such regulatory dilemmas and the fundamental ethical questions they pose for our social and personal rights, the thesis aims to revive the discussion by focusing on a reformative angle. Unlike most scholars who appear to be entirely focused on public regulatory framework when addressing big data concerns, this thesis intends to draw attention to the other side of the fence, which is enterprises' behavior toward personal data privacy and their indisputable impact in shaping the data protection and privacy laws' global enforcement. Thus, rather than approaching the issue from the state perspective alone, the thesis aims to draw attention to the oft-neglected aspect of Corporate Social Responsibility. In more specific terms, the thesis contributes towards creating a discourse that builds upon the strengths of CSR as the way forward in framing a more secure, efficient and workable data protection regime.

Therefore, the thesis contributes meaningfully to a live debate by opening new theoretical pathways and conceptual vistas to reimagine the future of data protection.

Chapter I: Public data protection regime in the age of big data

In this chapter, I will provide an overview of the GDPR data protection regime. I will discuss the rationale behind the GDPR and its structural design features. The chapter will assess the significance of the GDPR in the light of its own objectives. Such objectives include safeguarding of the personal data of the data subjects', and its overall impact on the preventing digital abuses in the data-driven world. The chapter also sheds light upon the key strengths of GDPR, and evaluates its success in enhancing data protection.

1.1 Background of the GDPR

The work of the European Data Protection Board highlights the dangers posed by the rising power of dominant Big Data corporations in the digital era. It highlights the risk that large datasets and 'sophisticated analytics tools' can lead to a greater economic imbalance between data-processing companies and data-feeding consumers (Article 29 Working Party, 2018). Their work highlights how such data-opolies clearly decrease the options of data subjects to seek alternative service providers. In this background, GDPR is seen to operate as a ray of hope to combat the power of such big technology firms, and to hold them accountable when it comes to respecting the end-user's privacy. Overall, the GDPR seeks to establish a consistent, all-encompassing approach to privacy breaches and mass surveillance for EU citizens.

GDPR is notable for creating a new rights-based framework. It's ambitious and at the same time, exhaustive in its scope. GDPR has been hailed as the holy grail of data protection at a global level. One among many of its uniqueness lies in creating a pan-continental system of enforcement and rights-network. The GDPR's legal basis is mandated in the article 8 of Charter of Fundamental Rights as well as in the article 16 of TFEU (Lee and Docksey, 2020).

GDPR is distinguished by its intention to reinforce and specify data subjects' rights and the obligations of those who handle and govern the processing of personal data, increase monitoring and reporting compliance powers with personal data protection laws, and provide sanctions for infringements in Member States(s).

Due to its unique standing in regulatory design and approach to data protection, the European Commission has hailed GDPR as "the gold standard" (EDPS, 2018) in data protection regulation and as "the most important development in 20 years". Enhancing rights, implementing new consent practices, and increasing resources and fines are cited by the commission as GDPR's innovative factors that pave the way forward for a greater assumption of responsibility by the organizations regarding Big Data. Regardless of praise or criticism, the General Data Protection Regulation (GDPR) is the world's leading data protection regulation, affecting legislative and corporate policies worldwide.

1.2 The guiding values of the GDPR

In terms of its basic nature, structure and defining key values, essentially, the GDPR is a set of seven key principles, which govern how data about individuals can be handled. Such principles of the GDPR are: lawfulness, fairness and transparency; purpose limitation; data minimization;

accuracy; storage limitation; integrity and confidentiality (security); and accountability ((Regulation (EU) 2016/679).

It is argued that GDPR's comprehensive grasp and its territorial reach makes it an important public regulatory model. It is also argued that GDPR is an important example of how the EU legal system is responding to the new and innovative digital technologies and is evolving to live up to the task of creating new rights and legal processes that accord with the rapidly increasing role of technology in our lives.

To support its highly ambitious regulatory aims GDPR comprises numerous unique features. Some such features being the generation of new rights and obligations concerning the purpose of which the data is to be collected, the way the data is profile, the new entitlement to refuse to be subjected to automated decision-making, rights concerning portability, as well as the right to be forgotten (Lee and Docksey, 2020). Likewise, apart from creating such rights, GDPR levels up the enforcement regime and creates new powers for supervisory authorities to monitor, investigate and implement the GDPR-related protection mechanisms — in a way that ensures EU-wide consistency and harmonization of GDPR laws (Lee and Docksey, 2020).

GDPR has also been a success at a different, more theoretical level. It has fundamentally transformed the people's idea of privacy and has had a massive impact in creating a greater awareness of privacy-rights in the public consciousness of the EU peoples. Moreover, by creating this new discourse, GDPR has led to a collaboration of various stakeholders such as states and private organizations and have mobilized them towards a common goal (Lee and Docksey, 2020). Therefore, based on this new discourse creation, GDPR has been hailed by many as a truly landmark achievement, one that has had an unprecedented effect on the data protection regimes at a global level. GDPR could thus be seen as a new flag-bearer of global standards in data and privacy regulation.

One key element of GDPR's value system is that it places extreme importance on deterrence. This is reflected in its strict approach towards non-compliance. For instance, GDPR imposes a disproportionate amount of penalties. Such fines and deterrence mechanisms, it could be argued, creates a robust regime for upholding of privacy (Green and Daniels, 2020).

Such a focus on deterrence is also reflected in the GDPR's creation of new supervisory authorities. This is considered to be one of its significant strengths. It is believed by some that the GDPR's creation of national agencies and empowering them in widest possible terms to enforce GDPR creates an unprecedented level of data protection regime.

For instance, some of such extensive regulatory powers given to supervisory authorities include: investigative powers: to seek information from the controller, processor, and where relevant, the controller's or processor's representative, to conduct investigations in the form of data protection audits, to inform the controller or the processor of any alleged violation of this Regulation, to obtain from the controller and the processor all personal data and information needed for the fulfillment of its tasks; and to enter any premises of the controller or processor, together with the equipment and means used for data processing, in conformity with Union or Member State procedural law (Lee and Docksey, 2020). Not only that, the GDPR also entitles supervisory authorities with corrective powers. These include, but are not limited to, issuing warnings to a controller or processor that proposed processing activities are likely to violate Regulation requirements, reprimanding a controller or processor where processing operations

have been infringed on; ordering the controller or processor to comply with the data subject's requests to exercise his or her rights under the Regulation, to order the controller or processor, where appropriate, to bring processing activities into conformity with the terms of the regulation in a particular manner and within a set period, to order the cessation of data flows to a recipient in a third country or to an international organization, (Lee and Docksey, 2020). It is believed that such wide investigative and corrective powers will encourage such agencies to apply GDPR in the most aggressive possible manner, with the effect that the data protection regime would be secured at European level.

Another key feature of the strict enforcement mechanism of GDPR is evidenced in its range of heavy fines upon non-complying organizations. An example of the high amount of penalties imposed by GDPR is that in cases of non-compliance with the GDPR provisions, up to 4% of the annual global revenue of the non-complying organization can be charged in fine, or 20 million euros, whichever value may be higher. It can be argued that such large fines not only have a deterring effect due to the high monetary value, but also because they leave a symbolic mark on the infringing organizations' reputation. Thus the GDPR, arguably also creates pressures upon the firms to comply by a culture of name and shame. A high fine imposed by the EU would undoubtedly be damaging to the organization's reputation in both the public eye as well as in the corporate circles [Green & Daniels, 2020].

However, despite its successes, GDPR's data protection leaves much to be desired. For instance, it has been noted that the newer technologies such as artificial intelligence, and machine learning etc. pose a continuing dilemma for the relevance of the GDPR and the ever-elusive issue of technologies evolving at a rapid pace in a way can be said to thwart even the most ambitious of GDPR's strategies (Lee & Docksey, 2020). Here, one may note that the GDPR may arguably be unable to apply to such technologies, and that its enforcement mechanism may soon have to give way to newer technologies, and that its data protection rights may not fit neatly with the rapidly evolving technological interface. Since such digital technologies impact on our social lives and are a marker of our modern identities in many ways, they raise important legal, ethical, social and political questions concerning human rights in the 21st century.

These characteristics have exposed the GDPR to critiques from scholars and commentators. For instance, commenting on the GDPR data protection approach, Ari Waldman notes: "[T]he law's veneer of protection is hiding the fact that it is built on a house of cards. Privacy law is failing to deliver its promised protections in part because the corporate practice of privacy reconceptualized adherence to privacy law as a compliance, rather than a substantive, task. Corporate privacy practices today are, to use Julie Cohen's term, managerial.''(Waldman, 2021).

1.3 GDPR's success in enhancing data protection standards

This section of the chapter delves into the protections and benefits that the GDPR regime has conferred upon the data subjects and consumers across the EU. However, instead of providing a bucket list of various advantages the GDPR confers upon consumers and businesses, this section discusses two key advantages that are most relevant to the issue of enforcement and implementation of rights. The chapter discusses the innovation of the GDPR to bring the right to data protection on a legal footing at a global level. And the creation of a level-playing field that makes the enforcement of data protection laws effective.

Firstly, the GDPR has a symbolic value in that it recognizes the right to privacy as a basic human right. This is important because the GDPR is the first major legislative piece at the global level that recognizes such rights at an international level. This is a remarkable achievement of the GDPR in that it also reflects the EU's zeal and vigor in updating its legal systems to meet the contemporary challenges posed by digital technologies. Moreover, the very pan-European nature of the EU's legislative instruments makes such rights as privacy and data protection widely available. This is a strength of the GDPR in that it breaks the traditional jurisdictional boundaries that may prevent the victims of data protection from achieving digital justice. Yet, the GDPR is widely considered a blueprint for data privacy, often referred to as the "gold standard" for international data protection (Buttarelli, 2016). Although the GDPR applies to the EU, its impact has been felt more internationally, and the potential of its regulatory model being adopted as a global standard has been extensively addressed (Greenleaf, 2018).

The GDPR represents the first binding instrument which implements extraterritorial measures to the traditional data protection law. Prior to the GDPR, the EU market was seen as an elastic market (Bradford, 2020). Bradford notes that this means that if an organization was faced with stricter regulatory regimes in a particular jurisdiction in which it operated, it could easily relocate to a different jurisdiction in order to take advantage of its laxer regulatory regime (Bradford, 2020). In this sense, the place of operation of the organization or the place of its market was seen to be an 'elastic target'. Thus, the firms would be able to switch jurisdictions, and that was seen as a major problem of enforcement. Such was the case because organizations could flee from the jurisdiction demanding stringent rights-friendly compliance (Hern,2018). Due to a lack of extraterritorial implementation of such laws, the firms could, arguably, with impunity, break the law of the stringent country and get away with it. Or at least, such firms could circumvent the rights-friendly regimes. This created a degree of polarization in that the influential organizations would move away from and concentrate in countries that were safe havens for organizations. However, the GDPR changed that picture.

In the same vein, it has been argued that the GDPR creates a new regime of rights and responsibilities, which are comprehensive and ambitious in terms of their scope and thoroughness. For instance, GDPR allows data subjects to be notified about the information that is being collected on them, the purpose of such collection, and the way in which it will be utilized (Green & Daniels,2020). Moreover, the GDPR allows data subjects to obtain a copy of the data that is collected concerning them. Moreover, they have a legal right to request correction where the data that is being held on them is incorrect. Likewise, in certain situations, they have a right to be forgotten (Green & Daniels, 2020). Moreover, in certain specified situations, they can prevent their data being used for some purposes, for certain (data to be transferred to third parties for marketing purposes). Likewise, data subjects can refuse to be subjected to an automated decision-making process (Green & Daniels, 2020). Finally, the the GDPR also acknowledges the right of data subjects to seek compensation. Any person who has experienced material or non-material loss as a result of a violation of the Regulation has the right to seek compensation from the controller or processor. Such a wide set of rights, it could be argued, are extensive and expand the legal horizons in terms of their human-right friendliness. It could be said that such an extensive set of rights create a new culture of data protection enforcement that encourages and obligates organizations to pay more attention to privacy and other data protection values and norms.

Moreover, such human-rights friendliness of the GDPR also evidences itself in its institutional design, which is often referred to as Privacy by Design. “The term “Privacy by Design” means nothing more than “data protection through technology design.” Behind this is the thought that data protection in data processing procedures is best adhered to when it is already integrated in the technology when created” (GDPR 2016).

This focus on privacy by design is also evident from a wide range of duties that the GDPR imposes upon businesses. For instance, the GDPR requires the creation of new supervisory authorities at both private level as well as the member-state level. At a private level, by requiring the organizations to have an infrastructure to hold, process, manage and safeguard data, the GDPR can be said to instill an ethos of data protection within the very essence of corporate thinking (Green & Daniels, 2020). For instance, the GDPR mandates how organizations shall prepare compliance reports in cases of breaches of privacy, and to report any breaches within 72 hours of such breach having taken place. Moreover, the GDPR maintains that in cases of Subject Access Requests, the data subject is unhappy with the way the organization has dealt with his/her request, the data subject has a right to get his request reviewed by the data controller who comes from the same organization (GDPR, 2016). This way, the GDPR, reconfigures the way the business models in digital sectors work, and incorporates in them a respect for privacy.

1.4 GDPR: Brussels Effect and the global standardization of data protection norms

The GDPR, as with some other EU law, has now moved towards what may be called as ‘inelastic targets’(Brandford, 2020). This means that EU law will prevail regardless of whether the firm is operating or located outside of the EU, as long as there is some territorial nexus with the EU. The GDPR regulates ‘elastic targets’ in the sense that the regulation applies to any good or service involving the usage of personal data irrespective of whether the data controller is or is not established in the Union as long as the data themselves refer to a citizen of the EU. Similarly, non-EU citizens can appeal to the European authorities if the company processing their data is in the EU (European Union, 2016, pp. 32-33). Therefore, under the GDPR regulatory regime, companies no longer could relocate a business to circumvent certain rules without losing access to the international market. Bradford considers this as one of the most prime examples of Brussels Effects.

As a case in point, it is helpful to consider here, the Facebook strategy. It appears that easing the burden of data processing under the GDPR, by moving part of the targets (those who are neither resident in the EU nor directly EU citizens) under a more lenient jurisdiction, is no longer an option. For instance, in 2018, Facebook announced that they would have moved more than 1.5 billion non-EU users under the responsibility of the American subsidiary, Facebook Inc. (in Menlo Park, California) (Hern, 2018). Despite the company’s claims that they will not change the privacy controls or service to the targeted users, it was highly debated that the measure would allow Facebook to significantly reduce its exposure to the higher fines prescribed by the EU law.

As Bradford notes, Brussels Effect refers to how the EU is exporting its policies across the world, without using coercion or direct threats. The Brussels effect is seen as an example of the EU's extension of soft power (Bradford, 2012).

Thus, GDPR, as Bradford notes, can be seen as an example of the Brussels Effect. Firstly, GDPR has an extraterritorial application. Secondly, the GDPR capitalizes upon the EU's authority and status as an economically advanced, human-rights friendly legal and political entity that arguably promotes rule of law, democracy, and good governance. As Bradford notes such factors help create a normative appeal for the EU and lends legitimacy and credibility to the EU's legislation and policies. Applying this to the GDPR, it can be noted that its extensive set of rights protection framework for data subjects and end-users allows it to be seen as a model of rights that is fit for export to other jurisdictions. In this way, the GDPR serves as an important tool for diffusion of EU's policies.

Due to the Brussels Effect, it could be noted that gradually there is a trend towards regulatory convergence and harmonization. This means that as more and more countries begin to emulate the EU's GDPR models, the countries' national models for data protection will begin to converge to similar, if not the same regulatory standards. This convergence at a global level matches the level of harmonization at an EU level. It is because the GDPR takes effect in all EU member states, and thus, any procedural and substantive differences in the data protection rights would have to give way to a relatively more uniform set of application and enforcement of data rights across all 27 EU member states. Such harmonization and convergence paves way for the constitution of a common legal scheme of protection.

Essentially, the GDPR intends to protect citizens against the misuse of their personal data. In particular, to ensure that they reach their purpose, the public privacy regimes design their framework on the basis of an evenly regulated market, where all organizations, businesses and firms are put in front of a single set of rules evenly enforced and that works consistently throughout the entire single EU market. As mentioned previously, the EU-wide application of GDPR has an effect of creating a level playing field for both the businesses and organizations on one hand, and end-users and data subjects on the other. This means that national or jurisdictional differences would not expose certain end-users to more deficient or less favorable rights. Likewise, from the perspective of businesses, such a level-playing field ensures that no business would be subject to a stricter regime of rights protection.

Such a principle of an even playing field enables a consistent application of laws, and this facilitates companies to operate under a uniform standards of norms, where all actors are given the same requirements and tools to comply with the laws. This will minimize the risk of giant tech companies abusing their market strength.

In conclusion, the creation of such a level playing field is one of the key strengths of the GDPR's privacy regimes since it makes the legislation enforcement effective, and as discussed previously makes it difficult for organizations to avoid their data protection obligations by simply relocating to a different jurisdiction.

1.5 The GDPR's limitations concerning enforcement and implementation barriers

In this section, I am going to discuss why and how the GDPR has been an underachiever, and have had less impact than it was arguably meant to achieve. In particular, I will talk about how the less than optimal impact of the GDPR can be traced to the difficulties it has faced due to issues of compliance, as well as due to the issues in enforcement.

As (Chander, Abraham, Chandy, Fang, Park, Yu, 2021), note, as is the case with other legal instruments, the legal framework on data privacy laws suffers from enforcement issues. The authors term it as an 'enforcement gap'. This term refers to an incongruence between the aims of the law, and the pragmatic application and enforcement of such laws in achieving their stated aims (Chander, Abraham, Chandy, Fang, Park, Yu, 2021). In short, the enforcement gap explains why laws, even after being enacted, failed to achieve the desired outcome. The enforcement gap can be attributed to the costs of complying with the GDPR for firms, as well as the enforcement costs and difficulties that the EU member states are faced with while giving effect to the GDPR (Chander, Abraham, Chandy, Fang, Park, Yu, 2021).

Although the GDPR has undoubtedly led to many improvements in data protection, it could be said that the real bite of the GDPR is missing. I will now discuss some of the reasons why such is the case.

Chander at el (2021) notes that the GDPR sets an extensive subject-specific framework of the amount of data that needs to be collected. It is certainly not an overstatement to suggest that the GDPR requires a complicated enforcement mechanism. The GDPR mandates that there must be a legal basis for processing of personal data. For instance, such a legal basis can come from consent of the data subject, or from a legal duty (Abraham, Chander, Fang, Park, Yu, 2021).

As the classic work of Zarsky (2016) in this field notes that the GDPR suffers from 4 major limitations concerning its enforcement and implementation (Zarsky, 2016). Such four major impediments means that GDPR stifles technological innovation and commercial enterprise. Firstly, the purpose for which data may be collected marks an important limitation in achieving GDPR's purposes. For instance, as discussed above, the narrowly defined legal purpose for collecting data, while enhancing data subjects' privacy, may, on the other hand, may also have a chilling effect on competition (Zarsky, 2016). In other words, the narrowly defined purpose for which data is collected may nonetheless discourage start-ups and other firms from gathering consumer information, and this may prevent them from entering new markets (Cennamo & Sokol, 2021). As an enforcement priority for the EU authorities, thus the GDPR fails to make much difference since large businesses, who already have access to a wider consumer base can amass a lot of big data, may actually be able use it strategically to redefine the terms of the market (without, however, committing a data abuse under GDPR) [Zarsky, 2016]. However, the small firms, whose potential for data privacy may not be high may actually be prevented from expanding their activities in digital platforms (Zarsky, 2016). In this way, 'purpose limitation' under GDPR can counterintuitively lead to potential data abuse by larger firms by focusing mostly on smaller firms (Zarsky, 2016).

Another problem with the GDPR's enforcement gap is due to data minimization. This term refers to the legal obligation upon the businesses to gather minimum possible data. While 'purpose limitation' restricts the purposes for which data may be gathered, the data minimization principle restricts the magnitude of data that may be collected. In GDPR, article 5(1)(c), states that the data to be collected should be ""limited to what is necessary" [GDPR article 5(1)(c)]. However, Zarsky notes, data minimization goes against the grain of 'Big Data Analyses' which mandates firms to collect as much data as possible to generate value and create more business activity (Zarsky, 2016). Such principle mitigates against collecting little data, retaining it for as short a time as possible and destroying it immediately afterwards (as required

under GDPR). Thus, Zarsky notes data minimization principle is an enforcement problem, since GDPR is being over-enforced (Zarsky, 2016). Arguably, such an over-enforcement casts doubts on the efficacy of GDPR's overall aims, and its relation with the freedom to conduct business (Zarsky, 2016).

Third problem with the GDPR's enforcement mechanism is its use of special categories. Special categories refer to a certain highly protected class of data, that is sensitive in nature, and requires an extra level of care in dealing (Zarsky, 2016).For instance, data such as the subjects' race, ethnic origin and sexual orientation, etc fall in this category. The creation of a separate category of data, that is special as opposed to other generic data categories, creates a problem (Zarsky, 2016). The concern here is that the special category of data mushrooms, as more and more data starts to be seen as personal, and highly sensitive (Zarsky,2016). For instance, the category of data pertaining to health and medical history may include data about the subject's purchases of certain recreational drugs, or certain medical products. Moreover, more and more of their purchases and transaction history via online shopping could for instance be seen as forming a part of data concerning 'health'. The problem of this mushrooming of categories is that soon the boundary between generic data and special category blurs in terms of implementing data protection since any meaningful divide between the two would be rendered superfluous (Zarsky, 2016). This, as Zarsky notes creates extra regulatory costs and burdens for the data handlers and on the whole, disincentivizes businesses. This creates problems of over-enforcement of the GDPR (Zarsky, 2016). Moreover, as Zarsky notes, this special category of data that requires special legal regime goes against the very logic of fluidity and swifitness (Zarsky, 2016). Moreover, as more and more data is being included in the special category, the distinction between generic and special category will blur to the point that all data will be treated alike at the lower threshold of generic data.

Similarly, the 4th major problem Zarsky notes with the enforcement and implementation pertains to automated decisions. Article 22 of the GDPR sets forth a legal rule that prevents a certain type of automated decisions to be made by the digital platforms (Zarsky,2016) For instance, credit applications and recruitment processes fall in this category. The GDPR allows data subjects to opt out of such processes, or require the presence of a human assistant, to help them process such applications. Zarsky notes that such processes interfere with the technological logic of Big Data, which in turn creates problems of implementation and enforcement (Zarsky,2016)). For instance, Zarsky notes how Big Data relies on automated processes to deal with data, and allowing subjects to require the presence of a human assistant would not only inevitably slow down such processes, but also add to the firm's costs and regulatory burdens (Zarsky,2016). Given the ubiquity of automated processes in digital markets, Article 22 of GDPR presents a real threat to the way innovative, new technologies operate in the 21st century. Thus, based on Zarsky's analysis, one may argue that the GDPR contains certain provisions that interfere with the logic and character of big data, and unsettles the technological interface of firms (Zarsky,2016)). The GDPR may thus necessitate businesses to change their technological interface and their business models. Such demands may seem to be too drastic, and could be seen as an overzealous attempt of using data protection laws to effectively rewrite the terms of business.

Moreover, it must be noted that the GDPR in its very enforcement mechanism imposes certain legal duties and regulatory expenditures upon businesses. Such high costs and time involved in dealing with multitude of requests may constrain firms from devoting time and resources to

their core activities (Chander, Abraham, Chandy, Fang, Park, Yu, 2021). For instance, GDPR requires organizations to have a certain data-handling capacity and personnel to deal with data-related requests, which are usually free. Thus, data subjects may be incentivized to make free requests, and impose demands upon the resources of the firm (Chander, Abraham, Chandy, Fang, Park, Yu, 2021).

Moreover, such a data-hander has to comply with all the legal obligations the GDPR imposes upon organizations, and this requires the organization to hire certain technical experts in this field. For instance, such experts would engage in risk assessment, and ensure the protection of subjects' personal data (Chander, Abraham, Chandy, Fang, Park, Yu, 2021).

Likewise, there are legal complications in defining who a data processor is under the GDPR and who a data controller is. Moreover, since the GDPR gives a legal right to access and request data held on them by an organization, this imposes time and cost constraints on the organizations. According to a study by IAPP, 56% of organizations that were surveyed noted that they faced difficulties in locating personal data that was unstructured (Chander, Abraham, Chandy, Fang, Park, Yu, 2021). In other words, the GDPR entitling the data subjects to request data from organizations mandate such organizations to process and catalog data in a way, which they may not otherwise do so (Chander, Abraham, Chandy, Fang, Park, Yu, 2021). Thus, the GDPR can be seen as imposing an artificial order or demand upon the resources, and database management capacity of the organizations.

When it comes to public enforcement of the GDPR by the EU member states, we see that the GDPR enforcing authorities in the respective member states are dissatisfied with the national budget for GDPR enforcement (Chander, Abraham, Chandy, Fang, Park, Yu, 2021).

Similarly, this dissatisfaction seems to grow owing to the rising number of data privacy complaints, especially the ones that involve giant tech firms, and/or involve trans-national cooperation involving more than 1 EU member state. Such a transnational cooperation mechanism inevitably increases costs and time in reaching decisions (Chander, Abraham, Chandy, Fang, Park, Yu, 2021). Moreover, such trans-national cases involves a systematic engagement with laws of more than one jurisdictions and this adds to the costs and resource-capacity requirements of national data protection agencies. For instance, it is noted that the investigation involving Cambridge Analytica lasted for more than 3 years, and the UK's data protection agency incurred more than 3 million USD (Chander, Abraham, Chandy, Fang, Park, Yu, 2021).

Likewise, it has been argued that the GDPR could encourage firms to hide their breaches of security rather than reporting them. It is because many organizations lack the necessary required expertise to monitor security protocols in cloud-based data management (Ismail,2017)

Thus, in sum, it could be argued that the GDPR is trying to apply broad regulatory fixes to regulate data protection. Such broad regulatory strokes cast the net wider, and creates a situation of overenforcement where organizations are disincentivized due to the sheer cost of compliance and the technical capacity-building as a result of the GDPR (Cennamo & Sokol, 2021).Thus, the GDPR has been rightfully described as having the unintended consequence of stifling innovation (Cennamo & Sokol, 2021).

Chapter 2: Personal data protection under self-regulation

The previous chapter of the thesis discussed the rationale, merits and limitations of the GDPR, and its structural design features. Since the thesis employs a comparative methodology, in this chapter, the thesis shifts attention from data protection public regulatory regime to the private enforcement mechanism. The purpose of the thesis is to provide a review of such private enforcement mechanisms as to provide grounds to reflect on their relative merits and demerits. However, the chapter also highlights how despite the significant differences between the GDPR and private enforcement mechanism, both of these are not mutually incompatible. Thus, this chapter suggests how the GDPR and private enforcement mechanism is complementary, rather than being a substitute.

2.1 An overview of private enforcement mechanisms

In comparison to public regulation, the self-regulation data protection system lacks hard rules, supervisory authorities, remedial sanctions, a legal basis for data processing, and other strict privacy features.

However, private data protection mechanisms include a new generation of privacy and consent services in which corporations adopt data privacy initiatives, their customers behave as ‘supervisory authorities’, and damaged reputation and trust amongst customers have been used as sanctions. One prominent private enforcement mechanism is Corporate Social Responsibility. The data protection private regulatory model, in tandem with corporate social responsibility, aims for a core business strategy approach. That is, businesses must view the need to respect individuals' data protection rights as an opportunity, rather than a burden.

Alternatively, rather than playing catch-up with legislation and consumer expectations, the data protection private regulatory model, in tandem with corporate social responsibility, aims for a core business strategy approach. (Balboni, 2020). That is, businesses must view the need to respect individuals' data protection rights as an opportunity, rather than a burden.

Making data protection rights a priority and part of their corporate social responsibility practices allows corporations to readily differentiate themselves from competitors, boost consumer confidence, and improve perceptions of the company's integrity.

2.2 Putting CSR and market incentives in perspective: The case of Apple’s iOS14 update

In this section, I will focus on the case of Apple software update (the release of Apple iOS 14). This recent privacy policy update, demonstrates how CSR practices not only provides an ethical face for the corporations, and to fulfill their social commitments, but more importantly that CSR allows firms to create value for themselves. Such value creation, can for instance, take the form of gains in reputation, and increases in sales. For instance, Apple's commitment to managing their operations ethically and in accordance with customer expectations has benefited Apple in numerous ways, including corporate brand enhancement, company image improvement, and revenue growth. Due to such gains, tech companies may be incentivized to protect consumer data.

Therefore, arguably the Apple 2021 software update present one such notable example of CSR initiatives (Hoppner & Westerhoff, 2021). The Apple, itself, has argued that this update is meant to increase the personal data protection for Apple users (Parizzo, 2022). This update prompts the users of iPhone and iPad whether they consent to the third-party apps on Apple to allow them to monitor their web activity. Such an initiative can arguably be seen as one illustration of a responsible data privacy initiative on behalf of Apple.

However, it has been strongly discussed that such a move by Apple is actually triggered by other incentives. As Charlie Munger famously notes that where there is an incentive, it induces an outcome (Colman, 2018). In this context, in order to understand what drives Apple to create such a privacy-enhancing feature, this thesis explores at its business model. Apple provides a wide variety of platform services such as Apple Music, Apple Pay etc. However, among all such services Apple offers, its main source of revenue is the App Store. This because seemingly Apple does not generate a significant proportion of revenue from ads (Gartenberg, 2019).

Thus, to increase its sales revenue, Apple has to focus on retaining customer loyalty. One such way of retaining customers is to lure them by offering them a semblance of security. By providing a more secure digital experience in terms of personal data protcetion, Apple is responding to the growing awareness among customers who are valuing their right to data protection as an important part of their use experience.

In fact, given that advertising contributes little to Apple's revenue, seemingly altering the opt-in policy does not represent either a difficult or risky business strategy to undertake. Because, while on the one hand, Apple risked market advertisement dollars (apparently not much), on the other hand, the motive was to impress Apple's clients, and consequently, acquire greater market share by responding to the trend of people seeking more privacy. Simply put, seemingly it is highly considered that the Apple's latest privacy incentive was designed to increase market share on behalf of its devoted loyal client base.

The influence of this CSR marketing strategy also finds parallels in Google's business strategy. Although Google, unlike Apple, derives majority of its revenue from advertisement on its search services, it still followed Apple’s lead in updating its privacy policy. Google has announced plans to block tracking by third-parties of users of Google services (Parizo,2022). This comes as a significant move given Google’s prominent place in the world browsing services market.

Thus, what we see here is that data-opolies are using CSR strategically for their commercial gains, while using data protection as a tool to attract and retain user base. Given the strong market position of Google and Apple, it is likely that other digital corporations will also follow their lead.

Moreover, it is noted by various researches that consumers’ perception of a business's reputation is more important than the substance of its policy (Scott and Cerulus, 2018). In this context, perhaps, Facebook’s reputation and trust journey, over years, demonstrate best the above findings.

Unlike Apple, Facebook paid a heavy cost for choosing to ignore data protection considerations. For instance, after the Cambridge Analytica scandal (which consisted of data breach of millions of accounts of Facebook users), Facebook’s revenue and reputation evidenced a sharp downfall. Concerning the incident, according to the Ponemon Institute,

Facebook users' trust in the corporation has dropped by 66 percent, and the company's share price has dropped by $70 billion as a result of reports that data analysis firm Cambridge Analytica improperly obtained data on tens of millions of Facebook users (Ponemon Institute, 2020). Thus, it is strongly established that the lack of concern about privacy of user data made Facebook suffer a heavy loss to its reputation.

Not surprisingly, Facebook, the company that owns platforms such as Facebook, Instagram, and WhatsApp, rebranded as Meta last year. Mark Zuckerberg, the founder of Facebook, stated that the rebranding was to signify that the firm was expanding out and was associated with more than one product (Zuckerberg 2021), however many others argue that Facebook was renamed Meta in the hope that the negative connotations associated with its original name would fade over time.

Regarding Facebook rebranding, Taina Bucher, author of the book Facebook, stated: "All of the bad news and political battles it is currently waging have to do with its social networking products, so releasing something wholly new – in their thoughts – is a chance to completely rebrand and start over, without changing much with the existing problematic products." (Bucher, 2021).

The example of Facebook reveals the importance of CSR in the modern world, where rapid technological developments are transforming our lives. In such an increasingly digital world, the firms face competitive pressure to respect data protection concerns of their users. Although CSR is a self-initiative, and is not legally binding, a firm that takes the concerns of its user's data protection likely is inevitably bound to risk suffering severe harm to its revenue and reputation as Facebook did.

Yet, based on Facebook's experience, one can argue that a responsible approach towards data protection is not simply a formalistic exercise. In other words, data protection compliance is far from merely being a tick-box exercise, because it has real reputational consequences that can threaten the very existence of the corporation.

Interestingly, CSR boasts of a new, and different regulatory approach. Instead of being driven by the threat of legal sanctions, and regulatory punishments, the corporations are being held accountable by their consumers.

Therefore, as a conclusion to this section, it may be noted that CSR as a self-regulatory mechanism is highly important. It allows firms to regulate their own conduct while having some discretion over the code of conduct they use to regulate their activities.

In the context of data protection, Facebook, Apple, and Google reveal how the corporations are mandated to adapt a more considerate approach. CSR practices on data protection concerns, must thus be seen as an important survival tool for corporations, even in the absence of hard, binding legal repercussions.

2.3 Merits of framing personal data protection under CSR

In this section, I am going to discuss how the GDPR, despite its strong commitment to ensuring meaningful consent by the data subjects, still fails to have the kind of impact it aims to have. This section notes how despite the stringent requirements of consent imposed by the GDPR, some, if not all, corporations are able to circumvent the GDPR requirements and engage in profiling activities. The fact that such practices still continue in contemporary times is a

testament to the fact that GDPR's protection is lacking in real terms. This section, therefore, makes a case for CSR to be adapted as a complementary strategy along with GDPR. The section also notes how CSR is beneficial for the corporations. Given the multiple benefits CSR provides, and the meaningful space it provides for a corporation to combine its own commercial interests with its ethical responsibility, it is argued that it could be the way forwards for personal data protection obligations to be incorporated under CSR models.

According to the GDPR provisions, the legitimate consent must be freely given, unambiguously, informed, and withdrawable at any moment (Article 7 of the GDPR). In the event of a dispute, the data controller must demonstrate that the subject truly consented to the processing activities (European Commission. (2018). In addition, the GDPR requires organizations to rethink how they acquire and secure data, placing transparency and commitment obligations on all parties.

However, it is evident that, even after the GDPR enforcement, companies are still legitimately carrying out quite extensive profiling activities based on broken privacy policies and meaningless consent. In this regard, the practice of dark patterns for privacy notices are constantly reported on by consumer protection organizations (Forbrukerrådet, 2019), white papers (European Data Protection Supervisor,2018),and various press (New York Times ,2016).

For instance, the Norwegian's Forbrukerrådet report by analyzing a sample of settings in Facebook, Google and Windows 10, shows "how default settings and dark patterns, techniques and features of interface design meant to manipulate users, are used to nudge users towards privacy intrusive options'' (Forbrukerrådet,2019).According to the report's finding, ''Facebook and Google's privacy policies include privacy intrusive default settings, misleading wording, giving users an illusion of control, hiding away privacy-friendly choices, take-it-or-leave-it choices, and choice architectures where choosing the privacy friendly option requires more effort for the users" (Forbrukerrådet,2019).

In contrast to the report's findings that the corporations' privacy friendly option necessitates greater user effort, the GDPR establishes that it must be "as easy to withdraw as to give consent" (European Union, 2016. Regulation (EU) 2016/679). This means if consent was obtained with "only one mouse-click, swipe of keystroke", withdrawal must be "equally as easy" and "without detriment" or "lowering service levels" (Article 29 Working Party, 2018).

In this context, given the meaningless consent and broken privacy notices that various studies have demonstrated over the years by measuring the influence of the GDPR on the collecting and processing of personal data, it is highly contended that neither the GDPR nor any other upcoming legislative framework will ever be able to successfully control our technology-driven environment while simultaneously flawlessly optimizing the advantages for citizens and effectively reducing risks for data subjects.

In fact, the European Data Protection Supervisor, the European Commission, and the Council of Europe have all stressed the importance of an ethical and value-based data processing approach as a goal of developing virtuous compliance that goes beyond the mandatory laws' requirements (Balboni, 2020).

Specifically, the latter stated that: "[t]the extent to which humans can enjoy their fundamental rights depends not only on legal frameworks and social norms, but also on the features of the

technology at their disposal. Recent discoveries of inappropriate use of personal data have driven the public debate on data protection to an unprecedented level. It is necessary that the shaping and the use of technology takes account of the need to respect the rights of individuals, rather than being driven exclusively by economic interests of few businesses." (Opinion 5/2018).

After all, the existing power imbalance between businesses as data collectors and individuals as data providers, and the alleged legislation's inability to remedy it, enhances even stronger the demand for businesses to engage in corporate social responsibility activities that positively affect both their long-term economic benefits and users' right to data protection.

From the standpoint of data protection, framing the data protection as CSR generates long term benefits to data subjects, businesses and entire society, as well. Beginning with the appointment of chief privacy officers (Awazu & Desouza 2004) to the publication of privacy policies on commercial websites (Sama & Shoaf 2002) to the adoption of CSR practices as a competitive advantage weapon, corporations have made substantial progress in recognizing the right to data protection as a priority and its great benefits, on doing so.

Therefore, the most innovative firms across the globe are approaching CSR more than just their ethical responsibility to community and the environment, but instead as an important strategic decision to accomplish their business goals (e.g., Kotler and Lee 2005; Lemon, Roberts, Winer, and Raghubir 2010; Mahoney, McGahan, and Pitelis 2009; Margolis and Walsh 2003; Porter and Kramer 2006).

CSR strategies have been shown to be so efficient that even the market leader can be reaped by another market challenger only on the basis of the latter's involvement in CSR activities, as opposed to those who are hardly aware. (Du, Bhattacharya, Sen, 2011).

This shift is explained in part by the intended attitude that customers show in favor of the market challenger, as well as the critical role that participation in CSR initiatives can play in transforming the nature of the relationship with the consumers from transactional to trust-based.

Moreover, in this data-centric society, data protection is being strongly recognized as a significant indicator of corporation credibility. Given the wide opportunity for companies to conduct business on the Internet, the issues of trust and trustworthiness play a strategic role (Hoppner & Westerhoff, 2021).

Among other factors, in the long term, corporations are able to gain competitive advantages merely based on the positive perception that its stakeholders have of it (Rindova and Fombrun, 1999)

Considering the value of personal data and the fact that the reputation is built and consolidated over time, and that reputation is highly dependent on perceptions, the businesses, more and more, are feeling the urge to embrace the consumer's push for expanded rights and access to their data.

Therefore, witnessing the incompatibility with the age of Big Data even of the strictest data protection legislation, such as the GDPR (Zarsky), the multi-faceted impact that multinational technology companies are having in our society, and the individuals' extremely increased demand for data protection, as Balboni suggests it is time go one step further, from data

protection by design to the 'fairness by design' concept (Balboni, 2020). Only doing so, the legal, ethical and other social dimensions of data protection would converge into a democratic digital society.

2.4 Data-opolies and the perils of self-regulation

This section discusses the problem generated by data-opolies and highlights the cons of self-regulation. In order to embark on such an evaluative exercise, this section discusses the issue of the above mentioned recent Apple App Tracking Transparency Police (Apple iOS 14 Update, 2021).It is suggested that such a focus on Apple's policies, and its review will contextualize the issues with data-opolies, since the reflections on Apple's policies can be applied more generally to such tech-giants in the ever-increasing digital age.

This policy, apparently, is argued that it is an improvement for providing Apple's consumers with the right to control the way their data is handled by third-parties apps. In particular, this privacy initiative is an "additional "verification check because even though the users might have consented to sharing their data with the app developers. Since it is the latter of the two steps, a refusal on this step means that it would override the earlier consent given to the app developer.

On the one hand, this feature has been hailed as enhancing the protection Apple provides to its users. Seemingly, this additional step acts as a safeguard and gives more powers to consumers to withdraw or override their earlier given consent.

Nonetheless, it is argued that such a feature is not as user-data friendly as it may seem at first (Hoppner & Westerhoff, 2021). There are several reasons for making such an argument. Firstly, a number of critical voices reflect that rather than transfer any real choice or power to consent to users, such transparency policy actually entrenches the already strong market power of data-opolies in digital markets. This means that tech-giants such as Apple can increasingly draw more and more users (and hence create network effects in their favor). Due to this new data-protection features, the traffic to Apple's ecosystem is likely to increase manifold.

Secondly, it is argued that Apple tightly controls the terms on which such request for information can be obtained by the app developers. This arguably creates a system where Apple can dominate, in fact, dictate the terms on which data is collected, and processed in this digital industry (Stucke, 2018)

Moreover, it is argued that because this additional permission-requesting step contains only a very basic format of providing consent (i.e., the only option being to say Yes or No), it fails to equate to meaningful consent even when a user clicks Yes to such request to being tracked. Under the GDPR rules, the consent to be meaningful requires provision by the app developer of more data and context as to what information is being collected, along with a justification. Hopner highlights that such is the case because EU law places great emphasis on empowering consumers to make informed decisions. Such an emphasis is disregarded by Apple, for instance, when it only allows users a Yes or No option, without explaining the ramifications of such choices. That is to say, without revealing consequences of saying yes or no, the end-users are not sufficiently endowed with any real capacity and choice to make decisions (Hoppner & Westerhoff, 2021)

Moreover, it could be argued that instead of letting third-parties (i.e., ad developers) collect all the sensitive data about users, Apple is redirecting the power to itself. This way, Apple like any true data oligopolist is (collectively with other such tech-giants) setting the rules for the entire industry.

Based on such problematic aspects of Apple's self-regulation regime, and its portrayal as a protector of digital privacy rights is contested. It is because, while Apple prevents other firms from engaging in dubious data-related practices, it relentlessly continues in such pursuits (Hoppner & Westerhoff, 2021)

Moreover, as a 'data-opoly', its unique market strength allows it (via such new transparency features) to actually lead the narrative on data protection. However, such a benign narrative disguises the more and more accumulation of power that results to Apple as a result of its new data-protection feature. Ironically, this new feature can thus be interpreted to imply that no one but Apple itself is allowed to track data users.

It is because, as noted by Hoppner, Apple's tracking policy is defined in a very narrow and biased manner. For instance, Apple's new data policy takes issue with data accumulated by third-parties, but makes no inroads into making transparent how it itself acquires First-party data. That is to say, "tracking only refers to the combination of data with data sets of different undertakings, i.e., of unassociated companies... Conversely, the combination of different data sets collected through different services within the same group of companies (so-called First-Party Data) is not covered" (Hoppner & Westerhoff, 2021) (Thus, data collected by Apple or products in Apple's ecosystem do(es) not prompt tracking permission, but the tracking prompt only appears as between end-users and their engagement with app-developers.

Moreover, such incremental accumulation of users' data creates network effects, and this means that the market for digital services tips in the favor of Apple (in other words, Apple's digital eco-system gets stronger). It is because, while other app-developers cannot access end-user data (Hoppner & Westerhoff, 2021)

As a result, Apple gets to have it all, and can then monetize it to third-party advertisers. Since it is a data-opoly, it does not face any significant barriers against doing so. As a consequence, more and more power accrues to Apple to continue to augment its market strength. This fierce competition against Apple's rivals for more and more users comes at the cost of privacy standards, which become more and more illusory, as a result.

This section concludes that Apple's case has broader significance for the regulation of data protection. As argued in the section, Apple's new data protection policy reveals tensions between privacy protection on one hand and the zealous competition on the other hand. Apple's new protection policy is illusory in terms of offering any better or substantive data protection. Such a new policy is thus a disguised attempt at drawing more and more big data to itself, and to retain its already strong market position (Stucke, 2018).

The case of Apple is thus illustrative of a wider trend in digital markets where dominant technology companies such as Facebook, Amazon, Apple etc. use new technologies for their own strategic purposes. As data oligopolies, one can expect a degree of tacit and implicit convergence on the technical standards they would set in terms of data protection. By portraying that the war is between the end-users and third-party ad-developers, Apple makes invisible its own share of detriment to consumer privacy. This could be seen as a typical

example of a data oligopolist claiming the narrative on data protection and pretending to be the champion of data protection standards, while disguising the massive inequality and disparity that exists between the end-users and Apple's significant power in the big-data ecosystem.

Conclusion

This thesis has engaged with critique of the data protection public regulation regime and of the data protection self-regulation regime. The thesis compared the schematic map, aims, ambition and enforcement strategies of the GDPR and self-regulation. The thesis discussed the promises and perils that underlie both such regimes in so far as they pertain to safeguarding the rights of individuals' on data protection and their impact on the overall data protection governance.

With this argumentative structure in mind, the first chapter discussed the data protection public regulatory regime under the GDPR. The chapter highlighted the main innovations that the GDPR has brought to the regulatory landscape in response to the challenges brought by big data. The chapter noted how the GDPR has succeeded to varying degrees in improving the data protection scene, for instance through the creation of a new rights-based framework.

Moreover, the second section of the chapter continued this discussion by examining the GDPR's provisions with an aim to evaluate their various strengths and weaknesses. Here, the main evaluative benchmark has been the GDPR's own enforcement goals. One such important yardstick being the protection of fundamental rights and freedoms of natural persons, in particular their right to the protection of personal data. The chapter concluded that, on the whole, the GDPR has been successful in creating a normative framework, which is, arguably, suitable for emulation globally.

The chapter noted that one key strength of the GDPR lies in its ability to harmonize the international legal protection of data protection towards a point of convergence that creates a level playing field.

The chapter highlighted how such a level playing field equally benefits consumers (end-users) as well as entities. However, the chapter also noted that the significant innovations brought by the GDPR must be weighed against the limitations such regime faces. Some such limitations pertain to the enforcement and implementation barriers, which arguably have a chilling effect on innovation and competition. Such is the case because on one hand, the logic of big data dictates that more and more data should be collected and processed so as to generate more value. While, on the other hand, the design features of the GDPR such as 'purpose limitation' limits firms from collecting more data. It could be noted that such restrictions discourage the firms from creating more value. This prevents them from offering more innovative services that may be better suited to consumers.

Moving on, while the first chapter focused on the data protection public regulatory regime, the second chapter discusses the self-regulatory mechanisms. This chapter introduced a self-regulatory data protection model, in particular, the CSR. The chapter discussed how big tech corporations such as Apple are impacting the data protection scene on a global level. In this context, the chapter discussed the initiatives taken by data-opolies such as Apple to apparently improve the end-user's data protection. Despite some positives brought by these initiatives, the chapter noted how such measures in fact increase the market power of data-opolies and

serve their commercial interests under the guise of end-user protection. Although self-regulation is not binding, the thesis noted that its importance as a private mechanism must be acknowledged, and that this could be a promising field of enforcement in the future.

On the whole, the thesis concludes that self-regulation and data protection regimes both have their advantages as well as their shortcomings. The thesis also notes that none of these mechanisms is perfect, and that both mechanisms complement each other. However, the future of these regimes seem uncertain since the data-centric world seems to be evolving in unpredictable ways. In the light of this, the findings of the thesis are significant in that they highlight the relativity of both models. The thesis is significant for reminding that in the complicated digital era, there is no single workable solution for resolving conflicts and situations arising out of the big data era. The thesis thus is valuable not because it conclusively resolves the debate, but that in broaching the subject, its humble reminder that no perfect solution exists, it is hoped, will give rise to more relevant questions rather than simplistic ones that portray either of the two models as a panacea. Therefore, the strength and significance of this thesis lies in its humble reminder of this fact.

Bibliography

Cooley, T. (. (1888). A treatise on the law of torts, or the wrongs which arise independent of contract. 2n edn. Chicago : Callaghan & Co.

Daniel J.Solove. (2006). A Brief History of information Privacy Law in Proskauer on privacy.

Jeremy H. (1994). The Right to Privacy and the Public's Right to Know: The Right to Privacy and the Public's Right to Know: The 'Central Purpose' of the Freedom of Information Act,46 ADMIN.L..REV.41.

Martin, K. & Nissenbaum, H. (2016). Measuring privacy: An empirical test using context to expose confounding variables. Columbia Science and Technology Law Review, 18, 176-218.

Martin, K. (2016). Data aggregators, consumer data, and responsibility online: Who is tracking consumers online and should they stop? . The Information Society. 32 (1), 51-63.

Martin, K. (2016). Do privacy notices matter? Comparing the impact of violating formal privacy notices and informal privacy norms on consumer trust online. The Journal of Legal Studies, 45(S2), S191-S215.

Rouvroy, A. (2016). “Of Data and Men”. Fundamental rights and freedoms in a world of big data. Strasbourg: Council of Europe, Directorate General of Human Rights and Rule of Law, T-PD-BUR .

Thomas. I & Westernhof. P (2021) Hofstede Insights Country Comparison, https://www.hofstedeinsights.com/country-comparison/ .

Roslyn. L & Julian. M (2019), The GDPR: What It Really Does and How the U.S. Can Chart a Better Course.

Maurice E. St * (2018), SHOULD WE BE CONCERNED ABOUT DATAOPOLIES?

Anu B. (2020), The Brussels Effect: How the European Union Rules the World.

Kenneth A.B & Deirdre. M (2015), Privacy on the Ground: Driving Corporate Behavior in the United States and Europe.

Lee. C & Bygrave. D (2020), The EU General Data Protection Regulation (GDPR): A Commentary 2020.

Daniel, S & Jeremy. G. (2020), Digital Governance: Leading and Thriving in a World of Fast-Changing Technologies.

Holvast, J (2009), History of Privacy, IFIP International Federation for Information Processing.

Greenleaf, G. (2018) Global Convergence of Data Privacy Standards and Laws: Speaking Notes for the European Commission Events on the Launch of the General Data Protection Regulation (GDPR) in Brussels & New Delhi .

Bradford, A. (2012). The Brussels Effect. Northwestern University Law Review, 107(1), 1-68. https://ssrn.com/abstract=2770634.

Bradford, A. (2015). Exporting Standards: The Externalization Of The EU's Regulatory Power Via Markets. International Review Of Law And Economics, 42, 158-173.

European Union. (2000), Charter of Fundamental Rights of the European Union. Official Journal of the European Communities, C 364(1). https://www.europarl.europa.eu/charter/pdf/text_en.pdf

Chander, A, Maeza, A, Chandy, S, Fang,Y , Park. D & Yu. I (2021), Achieving Privacy : Costs of Compliance and Enforcement of Data Protection Regulation, World Development Report & Macroeconomics, Trade and Investment Global Practice.

Cennammo. C & Sokol. D (2021), Can the EU Regulate Platforms Without Stifling Innovation? https://hbr.org/2021/03/can-the-eu-regulate-platforms-without-stifling-innovation,

Apple Ios 14 Update, (2021), https://support.apple.com/enus/HT211808#:~:text=iOS%2014%20updates%20the%20core,improvements%20to%20groups%20and%20Memoji.

Colmann. P (2018), Following the Money: "Show Me the Incentive and I'll Show You the Outcome" https://www.simon-kucher.com/en/blog/following-money-show-me-incentive-and-ill-show-you-outcome

Gartenberg. Ch (2019), 'HOW APPLE MAKES BILLIONS OF DOLLARS SELLING SERVICES' https://www.theverge.com/2019/3/20/18273179/apple-icloud-itunes-app-store-music-services-businesses

Parizzo. C. (2022), 'Will Google kill third-party cookies?', https://www.techtarget.com/searchcustomerexperience/tip/Will-Google-kill-third-party-cookies#:~:text=In%20June%202021%2C%20Google%20announced,in%20a%20post%2Dcookie%20world.

Mark. S & Laurens. C (2018), Meet Europe's New Chief Regulator of Data Privacy, Politico.

European Commission (2018) The GDPR: New opportunities, new obligations. Tech. rep., Publications Office of the European Union, Brussels, Luxembourg , https://ec.europa.eu/info/sites/default/files/data-protection-factsheet-sme-obligations_en.pdf

Forbrukerrådet (2019). Deceived by Design: How tech companies use dark patterns to discourage us from exercising our rights to privacy,

https://fil.forbrukerradet.no/wpcontent/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf

European Data Protection Supervisor (2018), EDPS Opinion on the legislative package "A New Deal for Consumers".

Singer. N (2016), When Websites Won't Take No for an Answer. New York Times, https://www.nytimes.com/2016/05/15/technology/personaltech/when-websites-wont-take-no-for-an-answer.html?mcubz=0&_r=0

[European Union. 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1. (2016), art 7(3)].

Balboni. P. (2020), DATA PROTECTION AS A CORPORATE SOCIAL RESPONSIBILITY, https://www.maastrichtuniversity.nl/data-protection-corporate-social-responsibility .

Romasnky, R & Noniska. I (2020), Challenges of the digital age for privacy and personal data protection.

Gstreinm. O & Beaulieu. A (2022) How to protect privacy in a data field society? A presentation of multiple legal and conceptual approaches, Philosophy and Technology.

Ismail. N (2017), Cyber security industry believes GDPR is 'stifling innovation', https://www.information-age.com/cyber-security-industry-believes-gdpr-stifling-innovation-123467262/.

Awazu. Y & Desouza. K (2004) 'The Knowledge Chiefs:: CKOs, CLOs and CPOs', European Management Journal, https://www.sciencedirect.com/science/article/abs/pii/S026323730400043X.

Sama. M. L & Shoaf. V. (2008) , Ethical Leadership for the Professions: Fostering a Moral Community, Journal of Business Ethics .

Kotler, P., & Lee, N. (2005). Corporate Social Responsibility: Doing the Most Good for Company and Your Cause, https://www.scirp.org/(S(lz5mqp453edsnp55rrgjct55))/reference/referencespapers.aspx?referenceid=3189881.

Raghubir. P, Roberts. J, Lemon. K & Winer. R (2010), Why, When, and How Should the Effect of Marketing Be Measured? A Stakeholder Perspective for Corporate Social Responsibility Metrics, https://www.researchgate.net/publication/247837541_Why_When_and_How_Should_the_Effect_of_Marketing_Be_Measured_A_Stakeholder_Perspective_for_Corporate_Social_Responsibility_Metrics .

Shuili Du, C. B. Bhattacharya, Sankar Sen (2011), Corporate Social Responsibility and Competitive Advantage:
Overcoming the Trust Barrier, https://pubsonline.informs.org/doi/10.1287/mnsc.1110.1403

Chang, E., Dillon, T.S., Hussain, F.K. (2005) : Trust and reputation relationships in service-oriented environments. In: Third International Conference on Information Technology and Applications (ICITA 2005), Sydney, NSW, vol. 1, pp. 4–14 (2005), 15.

Jøsang, A., Ismail, R., Boyd, C. (2007): A survey of trust and reputation systems for online service provision. Decis. Support Syst. 43(2), 618–644.

Rindova, Violina & Fombrun, Charles (1999), Constructing Competitive Advantage: The Role of Firm-Constituent Interactions. Strategic Management Journal?

Michael E.Porter & Mark R. Kramer (2006), Strategy and Society: The link between competitive advantage and corporate social responsibility,
Magazine: https://hbr.org/2006/12/strategy-and-society-the-link-between-competitive-advantage-and-corporate-social-responsibility .

Giovanni Buttarelli, 01 July 2016, The EU GDPR as a clarion call for a new global digital gold standard, International Data Privacy Law, Volume 6, Issue 2;
https://academic.oup.com/idpl/article/6/2/77/2404469?login=true .

Hern, A. (2018, April 19). Facebook moves 1.5bn users out of reach of new European privacy law. The Guardian. https://www.theguardian.com/technology/2018/apr/19/facebook-moves-15bn-users-out-of-reach-of-new-european-privacy-law.

Markey, S. E. (May 24,2018). Introduces Resolution to Apply European Privacy Protections to Americans,. https://www.markey.senate.gov/news/press-releases/senator-markey-introduces-resolution-to-apply-european-privacy-protections-to-americans.

Article 29 Working Party, 25 May 2018 , https://edpb.europa.eu/about-edpb/more-about-edpb/article-29-working-party_en

Adam Satariano, ,. (June 9, 2018). G.D.P.R, a New Privacy Law, Makes Europe World's Leading Tech Watchdog,. N.Y.TIMES,
https://www.nytimes.com/2018/05/24/technology/europe-gdpr-privacy.html.

Adam Satariano, (June 9, 2018). G.D.P.R, a New Privacy Law, Makes Europe World's Leading Tech Watchdog, N.Y.TIMES,
https://www.nytimes.com/2018/05/24/technology/europe-gdpr-privacy.html.

Bronwyn Howell. (August 6,2018). Data Privacy Debacle Down Under: Is Australia's My Health Record Doomed? .http://www.aei.org/publication/data-privacy-debade-down-under-is-australias-my-health-record-doomed/.

Bronwyn Howell. (August 6,2018). Data Privacy Debacle Down Under: Is Australia's My Health Record Doomed? . http://www.aei.org/publication/data-privacy-debade-down-under-is-australias-my-health-record-doomed/.

Scott, M. (Retrieved September 10,2018,). Cambridge Analytica helped 'cheat' Brexit vote and US election, claims whistleblower.

Ari Ezra Waldman, 13 Jul 2021, Data Protection by Design? A Critique of Article 25 of the GDPR Cornell International Law Journal, Vol. 53, Northeastern University School of Law Research Paper No. 411-2021, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3773143.

Apple's announcement on the tracking prompt released April 2021, https://bit.ly/3hDHwoq.

Schiff (AdExchanger), Apple WWDC 2020: A Version Of Intelligent Tracking Prevention Is Coming To The App World, June 22, 2020, https://bit.ly/3hi7HRm.