5-2020

The Cost of Big Data: Evaluating the Effects of the European Union's General Data Protection Regulation

Kara Rebecca White
kwhite85@vols.utk.edu

The Cost of Big Data: Evaluating the Effects of the European Union's General Data Protection Regulation

By: Kara White, Dr. Larry Fauver

Smith Global Leadership Scholar

Chancellor's Honors Program

Haslam College of Business

The University of Tennessee, Knoxville

Table of Contents

The Cost of Big Data: Evaluating the Effects of the European Union’s General Data Protection Regulation

By: Kara White, Dr. Larry Fauver

Abstract

In the 1990’s the World Wide Web was created, drastically changing the way we do business, communicate, and live our lives. Ten years later in the early 2000’s the dot com boom happened, and several years later, new technology giants emerged—like Amazon, Google, and Facebook. From this, we now face “big data” that promises to solve world problems, but has the potential to create turmoil and malfeasance. My research examines the impact of the General Data Protection Regulation (GDPR) enacted in the EU in 2016 on firm value using Tobin’s Q and CARs. Using regression analyses, I observe that Tobin’s Q increases post GDPR for firms required to conform to the regulation. Moreover, I find that certain industries see more of an increase in firm value (e.g., Technology Services and Research & Consulting Services) compared to other industries. When I examine CARs, I observe an average return of +0.13% for the EU firms around the enactment date (5-day window). The implications of this analyses suggest that the GDPR enacted in the EU to ensure data privacy and protection increased consumer trust in business and positively impacted firm value.

Keywords: data privacy, data policy, big data, GDPR

Introduction

Dating back to ancient times, data—best described as information collected for analysis—has always been recorded and used to aid in decision making. From notches in wood and marks in clay tablets to lists of IP addresses that clicked on a hyperlink and billions of Tweets, data collection and analysis has rapidly transformed along with technology and society itself. Now, data is considered as valuable as oil, which Clive Humby- founder of the global Customer Data Science company Dunnhumby and current Chief Data Officer of Starcount- proclaimed in 2006 (The Office of Clive Humby and Edwina Dunn, 2013).

Increased connectivity to the Internet, greater access to mobile devices, and an endless amount of digital services have all aided in the recent sky-rocketing growth of data in the world. Data is used for decision making through descriptive, predictive and prescriptive analytics and is especially heavily utilized in businesses considering the mass amount of data generated every day. In fact, the analytical profession of statistics alone has a projected job growth of over 30% according to the U.S. Bureau of Labor Statistics, which is 500% greater than the average projected job growth in 2019 of 5% (U.S. Bureau of Labor Statistics, 2020).

Because of this, the amount of data in the world and the use for data has exploded. With greater amounts of data, greater responsibility for the use of that data has also been present. For the first time in data's history, individuals and businesses are being challenged with the ethical implications of harvesting and utilizing data. Different policies are starting to come in effect all over the world—some by a company's own initiative, but most enforced by the government and regulators.

One of the largest data policies with the biggest outreach to get passed is the European Union's (EU) General Data Protection Regulation, referred to as the GDPR. According to the United Kingdom's Information Commissioner's Office, after four years of deliberation and lobbying, the GDPR was passed on April 26, 2016 and went into effect May 25, 2018 (ICO). According to the EU, the GDPR aims to look create "lawful, fair and transparent" data processing and give people the rights to their data (ICO).

Clive Humby from Dunnhumby and Starcount's statement that he proclaimed in 2006 did not gain much traction until ten years later, when academics and Chief Executive and Technology officers realized how much truth his statement held, such as Ginni Rometty—CEO of IBM, a Fortune 50 company with operations in data consulting. Similarly, ten years later, in 2016, the GDPR was announced. This is also the same year that the large data privacy scandal regarding Brexit and the United States' 2016 Presidential election with Cambridge Analytica came out (*The Great Hack,* 2019). Events regarding Cambridge Analytica turned out to be breakout news stories with Congress and Parliament getting involved into the politics and ethics of data. These events drew additional light to the news of the GDPR and how the GDPR changes everything in the worlds where data and business intertwine going forward.

The EU's GDPR is one of the first major data policies to be announced and enacted. The full reach of the GDPR is currently unknown, but the current literature suggests that it will have an impact on the future of research and data science, human rights and ethical computing, and the way businesses conduct operations regarding consumer data and data privacy. My research aims to quantify the cost of the GDPR on business, and the results indicate that the GDPR has a positive impact on business through increasing consumer trust in business and positively impacting firm value.

GDPR Description

According to the United Kingdom's Information Commissioner's Office, ICO, the GDPR is a strict data guideline that applies to both data controllers and data processors. The key difference between a controller and processor of data is that a processor is in charge of the actual gathering and harvesting of the data, while a controller is the point of the operation that decides on the purpose and use of the data. The responsibilities of the controller and processor could be placed on the same firm if they complete the additional duties of being a processor without outsourcing. However, if a firm does outsource any processing data operations, the GDPR holds them accountable to ensure that all contracts with processors comply to the new legislation (ICO).

The GDPR applies to any business that has operations in the EU, which would consist of all EU firms and any international businesses that have markets in the EU. The only exceptions to the data law is for national security purposes and data processing carried out by individuals purely for 'household' activities (GDPR, Articles 3, 28-31, Recitals 22-25, 81-82). Additionally, information about corporations, public figures, and the deceased do not constitute as personal data.

Personal data can consist of a multitude of information due to the large connectivity and Internet of Things that has grown in the world. Notably, names, emails, and IP addresses are a few of the objects that are considered to be personal data. However, personal data at its simplest definition is defined by whether or not an individual could be identified from the information. In cybersecurity fields, 'encrypted' data is typically a safe way to continue harvesting personal information, as the data cannot be traced back to an individual. Albeit, the GDPR considers data -even when identifiers have been removed- still personal data (GDPR, Articles 2,4,9,10)**.**

In contrast to the Data Protection Act of 1998, the GDPR adds more direct responsibility to the controllers and processors. Individuals persons and authorities can hold them accountable if the data or data methods have been jeopardized by the GDPR's regulations; this is known as the accountability principle. The seven key principles of the GDPR inspire the spirit of the data privacy movement and are key in understanding both the complexity and thoroughness of this movement. In Article 5 (GDPR) the seven fundamental principles of the GDPR are explained. **Appendix A** lists these seven principles.

To summarize these principles, every organization collecting data must have a 'lawful basis' or decent reasoning for collecting and using such data. The user must have clear and honest information about how his or her data is being processed and utilized, and the utilization of the data must remain the same as the stated permissions (no unexpected or misleading uses).

I chose to focus on the GDPR as it is a "new age" data policy that controls for best data practices within the newest technologies. Older data privacy laws such as FERPA (Family Education Rights and Privacy Act) and HIPAA (Health Information Portability and Accountability Act) are still important and useful, but outdated in the sense they do not account for the newer technologies and different ways that data is being used in various targeted advertisements and propaganda. The policy is extensive with seven principles that are a modern adjustment to the Data Protection Act of 1998. These seven principles are the lawfulness, fairness and transparency of data, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability. Those principles are the center of the GDPR and embody the new concept of data privacy rights. Not to be taken lightly, the GDPR could potentially cost a company, hypothetically, in at least one of two ways: through preparing and changing data collection and analysis processes for the GDPR or through a fine for not complying with the policy. All companies that operate within the EU, including international businesses that have operations in the EU, are expected to comply to the GDPR (ICO).

In an article by Stephen Dockery in the Wall Street Journal (2016), Dockery discusses the uncertainty of how the GDPR will change business and privacy rights. Some think the GDPR does not do enough to regulate data, some think the GDPR interferes too much; no one knows for sure how the GDPR will change the way firms operate. After years of negotiation a lot of the policy is left undefined or in vague terms - a problem that becomes extrapolated when the GDPR is translated into 24 different languages at minimum to support all countries in the EU. The two year grace period, where enforcement is more lenient, is a way for firms to work out any gaps in their compliance. The article also mentions that these firms must overhaul certain elements of their business, while monitoring the law as it being constantly refined and widely implemented into diverse organizations. Mary Hildebrand from law firm Lowenstein Sandler said, “Compliance with the GDPR for many companies will require extensive re-engineering.” The final effects of the policy could take years to crystallize as the policy is still evolving in the sense of operational definitions, though early effects are already being observed (Dockery, 2016).

The GDPR is the strictest guideline to ever be placed on businesses regarding the collection and use of data, which poses interesting and unexplored questions: How does data policy affect the annual costs of business, if at all? How does data policy affect different industries? Does the stock market react to data policy announcements? Similarly, does the stock market react to data policy enforcement dates? Is compliance to data policy rewarded by the market? In this paper, I aim to answer these questions by comparing and contrasting firm value and firms in the United States and the EU. Additionally, using daily stock price data, I evaluate the market reaction around key dates within the GDPR's announcement and official enforcement start date.

Literature Review

The central place for all updates on the GDPR can be found on the webpage of the Information Commissioner's Office, the ICO in the United Kingdom. The ICO has the purpose of advocating for the information rights of the public interest. One of their main interests, as stated by their official website, are to "promote openness by public bodies and data privacy" for people. The ICO is a non-departmental public body that is run by the Department for Digital, Culture, Media & Sport. Their website contains a multiple of resources and references; the most relevant information on the website contains biographical information on officers and the ICO organization, specific GDPR details and rules, organization compliance assistance and guidelines, and a database records of action that they have already taken against organizations that broke compliance with the GDPR.

While this news source has a heavy bias towards favoring data policy, the information and explanation that the ICO gives is necessary to understanding the complexity and far-reaching applications that the GDPR has on businesses and organizations. There is room for future analyses on the trends within the action that the ICO has already taken, which could be leveraged along with the insights already discovered in the effects of data policies. In addition to the background information that the ICO provides, the ICO also publishes recent data privacy and policy news and opinions. The ICO provides helpful context to the far-reaching discussing that GDPR has brought into newsrooms, our conversations, and multiple other facets of our lives.

An example of the GDPR infiltrating not just the news, but pop culture, is Netflix's documentary *The Great Hack*. Published in 2019, the documentary exposes the details of the political Cambridge Analytica scandal that affected both the 2016 US Presidential election and UK's Brexit. The documentary follows David Carroll- a Parsons professor- and his journey to get back his personal data from Cambridge Analytica. The majority of the documentary is a series of exclusive interviews with whistleblowers Brittany Kaiser and Christopher Wylie weaved together to tell the story of how Cambridge Analytica used Facebook data to entice people to make certain decisions. Containing a large number of interviews and first-person perspectives on the inside of one of the most famous data privacy scandals, this exposé elicits a new perspective on the controversy and need for data policies. This documentary, contrasted with other sources used in this research, provides a true story that illustrates the need for such data privacies and some background behind why data policies have come to light in the recent years. Additionally, the documentary provides an accessible and digestible way for non-subject matter experts to be involved in the ongoing data policy discussion that is plaguing our society.

In contrast to *The Great Hack*, “The Cookie Monster Strikes Back - The Latest GDPR-Related Decision of the EU Court” by Anita Vereb goes through a case study of a GDPR ruling regarding a German website, Planet49. The ruling was that data consent cannot be reached via a pre-checked consent checkbox. This stands for data that is and is not considered personal data. The article by Dr. Vereb provides a current example of the ever-evolving legislation with a simple to understand problem. The example she provides is not the only correction or addition to the GDPR, and I will continue to see it evolve over time. This case can be used to foreshadow up and coming rulings and applications as time goes on, especially in terms of the Internet and Terms & Conditions, which the GDPR will undoubtedly continue to shape.

Anne Bahr and Irene Schünder (2015) evaluate a different topic related to the notion that GDPR will likely have a big impact on the scientific and biomedical research industries. Their research in International Data Privacy Law concludes that firms that use medical data are expected to have increased difficulty complying with the standards of the GDPR due to the sensitivity of the data used in studies and new explicit use rules (i.e., not being able to reuse data from one experiment for another that might be closely related unless explicit permission is gathered). The academic article discusses the different protection levels via different industries. This a unique perspective on the intersection of health data and policies. When evaluating the effects of the GDPR by industry, this article helps to explain the differences in health, science, and research fields in contrast to general business. The article prompts an interest in evaluating not only EU versus the US in terms of differences due to the GDPR, but internal differences in the EU by industry-to evaluate what industries are more affected, if at all, by the GDPR more or less than others (Bahr & Shlünder, 2015). Similarly, scientists Luca Marelli and Giuseppe Testa in “Scrutinizing the EU General Data Protection Regulation” (2018) discuss the effects of the GDPR on scientific research. Marelli and Testa conclude that the GDPR will have large effects on future research projects due to not being able to reuse date for new projects and research. Due to the challenges that the GDPR proposes to the Scientific Research industry, the GDPR will ultimately be an accountability test for many firms and organizations. The challenges that the GDPR and the overall uptake of data policies will call for more ethics councils and internal controls within firms and organizations (Marelli & Testa, 2018).

According to “If the legislature had been serious about data privacy…” (2019), a published editorial in the International Data Privacy Law Journal, the true impact of the GDPR has been felt by firms as well as the individual consumer, worldwide-not just the EU-and in all industries (Kuner, Cate, Lynskey, Millard, Loideain & Svantesson, 2019). Specifically, paper debates the future of “Freemium” services, which is a popular pricing strategy where a service is free to the consumer, but the company either makes money through offering tiered levels of upgrades or through using the data and information provided by the consumer to generate a profit through miscellaneous channels. Even with the GDPR in affect, consumers must choose between using an online service and sacrificing their personal data or opting out of a service and keeping their data private. The GDPR at this time does not protect consumers making these choices or offer a clear path for one to still receive their desired level of data privacy while being able to access a service; this potential “loophole” will be affecting many consumers in all countries (Kuner, Cate, Lynskey, Millard, Loideain & Svantesson, 2019). On the same note, Peter Blume in 2014 debunked several myths regarding the GDPR at a time when the legislation was in the early proposal stages. Blume, an advocate for consumer rights, explores whether or not the GDPR will actually sustainably give consumers more data rights. According to Blume, the GDPR is seen as a fix to the issues of the old rules. For instance, the GDPR follows the Data Protection Directive, an EU directive adopted in 1995 that focuses on personal data processing underneath the privacy and human rights sector. Blume also states that while the GDPR is a necessary step to mature data law, that misuse is inevitable and that stricter legislation still needs to be proposed and approved. While the purpose of my research is to evaluate the financial impact of the GDPR, it is necessary to consider the overarching effects of the GDPR on consumers (Blume, 2014).

Observing the impact of the GDPR on the consumer and the financial impact on firms merely scratch the surface of the different lenses on which one can evaluate the reach and breadth of the GDPR. In “Impossible, unknowable, accountable: Dramas and dilemmas of data law” (2019), the authors from the University of Colorado Boulder’s Department of Anthropology present an argument on the social implications and dilemmas that data law can create. Focusing on the GDPR in the study, Cool, Bauer, Hoeyer, and Pickersgill worked with lawyers and legal scholars from Sweden to draft an argument focusing on the accountability principle within the GDPR. Cool argues that the accountability portion of the GDPR challenges researchers and data scientists to take different and more ethical approaches to their studies. Attempting to take different and “more ethical” approaches creates adverse effects on researchers and data scientists such as anxiety and hesitation (Cool, Bauer, Hoeyer & Pickersgill, 2019).

A social science perspective is valuable when attempting to understand the effects of the GDPR - even from a sole cost standpoint. Cool, et al. concludes that some effects of strenuous data policies can be destructive for employees and work cultures. These costs are opportunity costs that should be considered when evaluating the different ways that the GDPR can “cost” a business. Alternatively, Franklin (2019) defends in the *International Financial Law Review* that the GDPR is an improvement, rather than strictly a cost, to many data processing and research practices. Franklin discusses how the GDPR affects artificial intelligence practices and innovation. While our research aims to pinpoint the costs of effects of the GDPR on firms, the GDPR’s potential to impact innovation in machine learning and data mining is one area in particular that could hinder productivity, profitability, and, as Cool discusses, the mental health of researchers. Franklin deduces that the GDPR does not hinder innovation, but rather keeps innovation in check with human rights and ethics in the ever-emerging field of data science. Albeit, Franklin’s claim seemingly supporting the GDPR, he admits that the “question of ethics” demands to be studied on an ongoing basis. Franklin also controversially states that he does not observe a need for GDPR reform, which is in direct contrast with the ICO’s statements on the GDPR’s evaluation period and constant proposed additions (Franklin, 2019).

The ethics of computing and data mining is a topic that has gained traction along with the spread of these fields and will not be going away any time soon. Inverardi (2019)- a professor in the Department of Information Engineering Computer Science and Mathematics at the University of L’Aquila, Italy evaluates the European perspective on responsible computing in an academic journal. The EU is one of the first and few places to be considering the ethics of data privacy and taking action against certain claims. Compared to the rest of the world, Europe is actively taking action with human-centered regulations. “The European Perspective on Responsible Computing” by Inverardi (2019) states:

> “From a regulatory standpoint, the GDPR was entered into application throughout the EU in May 2018. Article 1 states that: ‘Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.’
>
> The GDPR aims to give individuals control over their personal data and to provide a unifying regulation within the EU for international business. It states data protection rules for all companies operating in the EU, whether they are established in the EU or just operating inside the EU. This regulation forces controllers of personal data to shape their organization and their processing systems in order to implement the data protection principles. As already mentioned, GDPR is the most advanced regulation about personal data operating in the world.”

As a leader in data privacy regulations, Europe is heavily influencing technology companies. New and future legislations are one route of influence, and another is that the consequences of non-compliance with the GDPR are already being observed. Fines and action are being taken on companies that do not comply with the GDPR; companies as big as Google and smaller companies are being effected (“Why Big Tech Should Fear Europe”, 2019). Google was fined 57 million US dollars under the GDPR for not properly disclosing to consumers how their data was being collected across the multitude of services that they offer (e.g., YouTube, Google Search). While the Google fine was the largest yet from the GDPR, the fine is still lower than the maximum fine allowed from the GDPR, which is up to 4% of total global revenue; the maximum fine for Google would be approximately increase the previous fine by a factor of 70 ("Why Big Tech Should Fear Europe", 2019).

The large fine that Google faced is not alone and will not be the last fine that we observe from the GDPR. Partner at the London offices of CMS, Cameron McKenna Nabarro Olswang LLP, Laurence Kalman is experienced in law and regulatory compliance and takes a look into the one-year aftermath of the GDPR in "New European Data Privacy and Cyber Security Laws" (2019). Kalman mentions that as the GDPR and NISD- Network and Information Security Directive-are merely in their infancy, but will be causing an impact for a long time to come. The EU is setting a golden standard for data privacy, hardly rivaled by the select countries with data policies that are not as stringent as the GDPR. The US is falling behind in terms of data policy. Kalman (2019) discusses:

> "There are also signs that U.S. consumers look longingly at the protections available in the EU. According to a survey conducted in April 2018 by Janrain, the customer profile and identity management software provider, 68% of respondents wanted a GDPR-like law in the U.S. Some 38% identified their top priority as the ability to control how their data is used, while 39% focused on the right to require organizations to delete their data."

The EU's GDPR is the first of many rigorous data policies that have effects on business models and advertising norms, the future of research and data science, and human rights and ethical computing conversations. My research aims to quantify the cost of the GDPR on business through two ways: by observing the change rate of spending on key areas of the financial statements and by observing the market reaction to the announcement of the GDPR. My research answers these questions by evaluating financial data for firms in both the EU and US overtime and by assessing the market reaction via the stock market around the announcement of the GDPR.

Financial Statements Analysis

Methodology

To evaluate the effects of the GDPR on the cost of doing business, our research examines a total of 6,960 unique firms from the EU and compares them to the 4,739 unique firms from the US. The financial and accounting data are obtained from Worldscope and DataStream using Thomas Reuters WRDS, with firms from countries not in the US or EU removed. A firm was classified as belong to either the EU or the US. **Table 1** in **Appendix C** illustrates the spread of unique firms by grouping (EU or US) and year (2014-18).

In the analysis, the main variable of interest is firms in the EU between 2016-18. To serve as controls to this analysis, I evaluate the US firms in the same 2016-18 time period. The time period of interest, 2016-18, serves as a date range which covers the announcement and enforcement of the GDPR which was enacted on EU firms; I expect to observe early implications of the GDPR on financial statements from this particular date range.

To evaluate the change rates on key areas of financial statements, the average and median percent change by each financial area from 2016 to 2018 was calculated separately for the EU and US firms.

After comparing and contrasting EU and US firms based on reported financials, I aim to observe the affects that the announcement and early enforcement of the GDPR had on firms' financial statements. The cost of preparing for such a regulation that overhauls data privacy standards is unknown. Using data is a necessary operation in any firm, and through this analyses, I hope to gauge how and where the GDPR cost firms.

Univariate Analysis

Appendix C Table 2 illustrates the mean percent change and median percent change in spending by different functional areas of financial statements for firms in the EU and US from 2016 to 2018.

There is a notable difference in the average change rate of Staff Costs between EU and US firms. EU firms' average expenditure increase for Staff Costs is 72%, while the US during the same period is 17%. The median average expenditures are much more similar, around 7% for both EU and US firms. This indicates that the EU change rate for Staff Costs is highly skewed to the higher end, with some firms having dramatic increases in Staff Cost expenditures.

Additionally, the EU firms have exceptionally high average change rates in PPE and Development Cost spending. PPE costs rose on average 107% from 2016 to 2018 (median was 5%); this also indicates that the change rate for PPE expenditures is highly skewed to the higher end. The US firms see a similar pattern in 2016 to 2018 with the change in spending for PPE with a mean of 125% and median of 6%. Similarly, Development Costs grew 148% for the EU on average (median of 8%). The US firms' Development Costs grew only 16% on average with a median of -32%, indicating that Development Costs did not change drastically and likely were smaller for a lot of firms.

Evaluating the average change of Tobin's Q (defined as the ratio of the total market value of the firm over the total asset value of the firm) between the two groupings, I observe that in the control analysis EU firms had a higher change in valuation than the US. The EU firms on average had a change rate of -1% (median of -2%), while the US firms on average had a change rate of -7% (median of -5%) for the 2016-18 time period.

Then I expanded the analysis of Tobin's Q to evaluate the change in Tobin's Q in different industries using their SIC codes. This analysis only considered EU firms, shown in **Table 3** in **Appendix C**.

In **Table 3** in **Appendix C**, the percent change in the mean of Tobin's Q for EU firms changes in the different SIC groupings in a range from (-1.18%) to 11.95%. The biggest increases are seen in the following industries: Lodging Services, Mining, and Technology Services. The only areas with negative percent changes in the mean of Tobin's Q are Retail Trade and Advertising

Services. Additionally, two specific areas of interest- Technology Services and Research and Consulting Services- observe a positive percent change of means, 8.02% and 6.45% respectively.

Regression Analyses

Lastly, I quantified the impact of the GDPR on Tobin's Q through a regression analysis with Tobin's Q as our dependent variable with the goal of determining how the GDPR impacts firm value. The variable used to determine this is the *POST* variable. The *POST* variable determines whether or not the firm is positively or negatively affected by the GDPR (i.e., *POST* is defined as the firm is in the EU and year is between 2016-18). The fit of our regression is described in **Table 4** in **Appendix C**. In our regression model, 14% of the variation in Industry, natural log of Total Assets, ROA, Country, and *POST* describe the variation in Tobin's Q. The results of our model are statistically significant.

I conclude that the regression model I ran on our sample data fits the data better than the model with no independent variables. **Table 5** in **Appendix C** contains the specific results of the model by the intercept and variable. In **Table 5**, I observe the impact on valuation from the GDPR through *POST*.

POST is statistically significant and positive, indicating that after controlling for the size of the firm, the inherent initial differences between US and EU firms, and Industry, that the GDPR positively impacts and increases firm value for the EU firms.

Market Reaction (CARs)

Methodology

To gauge how the market responds to the news of the GDPR, cumulative abnormal returns (CAR) were calculated for every firm in both the EU and US around a 5-day window (-2, 2) for April 26, 2016. April 26, 2016 is significant to the study, as that was the day for the official announcement of the GDPR. The US firms serve as the control group, as the GDPR is currently only enacted in the EU.

The CARs found indicate whether or not the reaction from the stock market was different than what was expected (i.e., more positive than expected, more negative than expected, or as expected). I also ran and evaluated a Welch Two-Sample t-test of means on the CARs for EU and US firms to test for the statistical difference in CAR for EU versus US firms.

Market Reaction (CARs) Results

To gauge market reaction to the announcement of the GDPR, I evaluated the average cumulative abnormal return (CAR) for the EU and US firms within the (-2, 2) window for the announcement date of the GDPR — April 26, 2016. **Table 6** in **Appendix C** shows the average of the CARs and the standard deviation of the CARs.

The EU firms had an average CAR of 0.13%, which indicates that the stock market returns for the 5-day (-2, 2) time period were a positive 0.13% above what I would expect. The US firms within the same 5-day window had an average CAR of -0.5%, indicating the market reacted more negatively than what was expected.

To quantify the differences in CARs between the EU and US in the time window, I ran a Welch Two Sample t-test of the means, illustrated on **Table 7** in **Appendix C**. The results were not statistically significant, and I cannot confirm that there is a statistical difference between the market reactions for the EU firms and US firms.

Limitations

Through two separate analysis: the financial statements analysis and the market reaction study, this research attempts to gauge and understand the effects of the GDPR on the cost of business and firm outlook. While I take two separate approaches in attempt to weave a better picture of the delicate fragments in the story of ever-changing business operations in regard to personal privacy and data, our approaches are not all-encompassing and do not fully explain every phenomena in the new age of data and data protection.

One major limitation that this study faces is the ability to only use the financial information of public firms. The financial data from public firms was both useful and necessary in completing the studies and getting an understanding of the early effects of the GDPR, however, more of the story could have unfolded with additional data from private firms-of which I did not have access to and which are still expected to comply and are impacted by the GDPR. Without having access to private firm data, I believe that there is additional valuable information in their financial reports and the market value of their firm, which is respectively not publicly published or reflected through prices of stocks.

Additionally, the results of this study are affected by the way the control data was set up. Our control data was based off of countries in the US, and I chose not to compare and contrast with any other countries. I did this as the US and EU are similar in size and power, however there are still limitations in this study through only observing the EU and comparing these firms to firms in the US.

Lastly, the study fails to account for other events in the world. Namely, the Brexit debate that coincides with the dates around the GDPR announcement and enforcement. Brexit is a national debate regarding the UK's decision on whether or not to leave the EU in the UK which ultimately will affect all of the EU and likely other places as well. The effects of the Brexit debate and decision cannot be ignored, but should rather be considered when also looking at the way the GDPR is changing the landscape of business, data privacy, and human rights.

Conclusion

After analyzing both the impact of the GDPR on the cost of firms as well as the market reaction, the announcement and implication of the GDPR improves firm value. The implications of this observation suggest that the GDPR enacted in the EU to ensure data privacy and protection increased consumer trust in business.

For further implications of this study, it would be interesting to evaluate the why behind why the GDPR has increased consumer trust in business: Is the same true for other data policies? Does consumers' trust change after an incident or breach in data policies? Would there be a different observed impact if this study was performed several years later? Will the positive impact of the GDPR on firm value last over the years, as data policies become a normal requirement?

Overall, our study contributes to the ongoing conversation and literature regarding the impact of General Data Protect Regulation, and other data policies of its kind, on the cost of doing business in terms of firm financials and market reaction.

Appendix

Appendix A: GDPR Principles

In Article 5 (GDPR) the seven principles are laid out as follows:

> (a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');
>
> (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');
>
> (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

Appendix B: Variable Definitions

Variables of Interest

Tobin's Q: Total Assets minus Book Value of Equity plus Market Value of Equity divided by Book Value of Total Assets ; all amounts were in US Dollars

POST: Indicator variable equal to one for firms affected by the GDPR (Grouping equals EU and Year is in 2016-18)

Control Variables

Log of Total Assets: Accounts for the size of the firm

ROA: Return on Assets, calculated as the ratio of Net Income / Total Assets

Country = EU: Indicator variable equal to one for firms that are in the EU

SIC = *Industry*: Indicator variable equal to one for firms that fall into the respective industry category of the following groupings: Mining, Construction, Manufacturing, Transportation and Communication, Wholesale Trade, Retail Trade, Finance and Insurance, Lodging Services, Advertising Services, Technology Services, Health Services, and Research and Consulting Services. The Agriculture Industry is the reference level.

Appendix C: Tables

Table 1 - Data Description

	Number of Unique Firms	
Year	**US**	**EU**
2014	3604	5623
2015	3558	5369
2016	3361	5341
2017	3188	5174
2018	2979	3434
Total Unique Firms	**4739**	**6960**

Table 2 - Univariate Analysis: Growth Rate from 2016-2018 by Area

	EU		US	
	Mean	Median	Mean	Median
Staff Costs	72.45%	9.52%	17.12%	14.39%
R&D Expenses	10.31%	6.86%	19.14%	7.14%
Operating Expenses	10.03%	9.36%	16.25%	13.69%
Current Assets	40.22%	10.05%	17.68%	10.77%
PPE	107.73%	4.70%	125.20%	6.49%
Development Costs	147.61%	8.07%	16.08%	-32.06%
Material Expenses	42.52%	12.99%	20.78%	14.44%
Net Sales	240.58%	16.18%	25.56%	15.03%
Net Income	5.71%	5.60%	-25.34%	10.62%
Tobin's Q	-1.00%	-1.99%	-6.94%	-5.42%

Table 3 - Tobin's Q for EU Firms by SIC Group

SIC Group	Median Tobin's Q of Control 14-15	Mean of Control 14-15	Median of 17-18	Mean of 17-18	% Change of Means
Agriculture	0.9897549	1.094291	1.054928	1.138654	4.05%
Mining	0.978346	1.065571	1.08917	1.17322	10.10%
Construction	1.067584	1.114713	1.134375	1.173082	5.24%
Manufacturing	1.26973	1.343588	1.328103	1.40033	4.22%
Transportation and Communication Services	1.167185	1.244906	1.220095	1.27352	2.30%
Wholesale Trade	1.147342	1.244655	1.214406	1.276766	2.58%
Retail Trade	1.252571	1.355477	1.232694	1.339518	-1.18%
Finance and Insurance	1.001046	1.059061	1.01151	1.071835	1.21%
Lodging Services	0.9013937	0.948607	1.032872	1.061955	11.95%
Advertising Services	1.323804	1.395567	1.288395	1.375001	-1.47%
Technology Services	1.363719	1.431004	1.523104	1.545757	8.02%
Health Services	1.328856	1.379863	1.319029	1.391117	0.82%
Research and Consulting Services	1.36124	1.422438	1.510374	1.514123	6.45%

Table 4 - Regression Model Fit

Model Results					
R-Squared	Adj R-Squared	F-statistic	p-value of Model	DF	Residual Standard error
0.14	0.1397	423.4	< 2.2e-16***	41604	0.4218

Table 5 - Regression Model Results

	Estimate	Std Error	t value	Pr(>|t|)
(Intercept)	0.8823121	0.0292278	30.187	< 2e-16***
POST	0.03732016	0.0053864	6.929	4.31e-12***
ln(Total Assets)	0.0177258	0.009101	19.478	< 2e-16***
ROA	-0.0005998	0.0003073	-1.952	0.05094 .
Country = EU	-0.1408803	0.0052768	-26.698	< 2e-16***
SIC = Mining	-0.0700890	0.0254088	-2.758	0.00581**
SIC =Construction	0.0006250	0.0263977	0.024	0.98111
SIC = Manufacturing	0.2339971	0.0237089	9.870	< 2e-16***
SIC = Transportation and Communication	0.0930669	0.0244392	3.808	0.00014***
SIC = Wholesale Trade	0.1126652	0.0262861	4.286	1.82e-05***
SIC = Retail Trade	0.1970973	0.0255021	7.729	1.11e-14
SIC = Finance and Insurance	-0.0966766	0.0237643	-4.068	4.75e-05***
SIC = Lodging Services	-0.0730152	0.0304425	-2.398	0.01647*
SIC = Advertising Services	0.2381371	0.0272657	8.734	< 2e-16***
SIC = Technology Services	0.3528986	0.0245399	14.381	< 2e-16***
SIC = Health Services	.2107501	0.0281285	7.492	6.90e-14***
SIC = Research and Consulting Services	0.3498376	0.0262038	13.351	< 2e-16***

Table 6 - Market Reaction: Cumulative Abnormal Returns

Grouping	N	Average CAR	SD of CAR
EU	5005	0.13%	0.2349
US	3446	-0.50%	0.0593

Table 7 - Market Reaction: Welch Two Sample t-test

EU CAR Mean	0.13%
US CAR Mean	-0.05%
95% Confidence Interval	[-0.51, 0.85]
P-Value	0.618

References

Bahr, A., & Schlünder, I. (2015). Code of practice on secondary use of medical data in European scientific research projects. *International Data Privacy Law, 5*(4), 279–291. doi: 10.1093/idpl/ipv018.

Blume, P. (2014). The myths pertaining to the proposed General Data Protection Regulation. *International Data Privacy Law, 4*(4), 269–273. doi: 10.1093/idpl/ipu017.

Cool, A., Bauer, S., Hoeyer, K., & Pickersgill, M. (2019). Impossible, unknowable, accountable: Dramas and dilemmas of data law. *Social Studies of Science (Sage Publications, Ltd.), 49*(4), 503–530. https://doi-org.proxy.lib.utk.edu/10.1177/0306312719846557.

Dockery, S. (2016, April 25). Uncertainty Abounds in Europe's Data Privacy Overhaul. *Wall Street Journal*. Retrieved from blogs.wsj.com/riskandcompliance/2016/04/25/uncertainty-abounds-in-europes-data-privacy-overhaul/?mod=searchresults&page=1&pos=14.

Fauver, L., Hung, M., Li, X., & Taboada, A. G. (2014). Board Reforms and Firm Value: Worldwide Evidence. *SSRN Electronic Journal.* doi: 10.2139/ssrn.2607785.

Franklin, J. (2019). GDPR has kept AI ethical despite concerns. *International Financial Law Review*, N.PAG. Retrieved from https://search-ebscohost-com.proxy.lib.utk.edu/login.aspx?direct=true&db=bth&AN=139213623&scope=site.

GDPR - Official Legal Text. (n.d.). Retrieved March 5, 2020, from https://gdpr-info.eu/

Information Commissioner's Office. (n.d.). Retrieved March 5, 2020, from https://ico.org.uk/.

Inverardi, P. (2019). The European perspective on responsible computing. *Communications of the ACM*, *62*(4), 64–64. doi: 10.1145/3311783.

Kalman, L. (2019). New European data privacy and cyber security laws. *Communications of the ACM*, *62*(4), 38–38. doi: 10.1145/3310326.

Karpoff, J. M., Lee, D. S. S., & Martin, G. (2005). The Cost to Firms of Cooking the Books. *SSRN Electronic Journal*. doi: 10.2139/ssrn.652121.

Kuner, C., Cate, F. H., Lynskey, O., Millard, C., Loideain, N. N., & Svantesson, D. J. B. (2019). If the legislature had been serious about data privacy …. *International Data Privacy Law*, *9*(2), 75–77. doi: 10.1093/idpl/ipz006.

Marelli, L., & Testa, G. (2018). Scrutinizing the EU General Data Protection Regulation. *Science*, *360*(6388), 496–498. doi: 10.1126/science.aar5419.

Satariano, A. (2019, January 21). Google Is Fined $57 Million Under Europe's Data Privacy Law. Retrieved from https://www.nytimes.com/2019/01/21/technology/google-europe-gdpr-fine.html.

The Great Hack. (2019). Retrieved from netflix.com.

The Office of Clive Humby and Edwina Dunn - the future of customer engagement. (2013). Retrieved March 5, 2020, from http://www.humbyanddunn.com/.

U.S. Bureau of Labor Statistics. (2020, February 26). Retrieved March 5, 2020, from https://www.bls.gov/.

Vereb, A. (2019, November 4). The Cookie Monster Strikes Back – The Latest GDPR-Related Decision Of The EU Court. *Mondaq Business Briefing*. Retrieved from https://global.factiva.com/ga/default.aspx.

Why Big Tech Should Fear Europe. (2019, March 23). *Economist*. Retrieved from https://www.economist.com/leaders/2019/03/23/why-big-tech-should-fear-europe.