Does Data Privacy Regulation Only Benefit Contracting Parties? Evidence from International Digital Product Market

Ziru Li
Thunderbird School of Global Management
Arizona State University
ziruli@thunderbird.asu.edu

Gunwoong Lee
Business School
Korea University
leegw@korea.ac.kr

T. S. Raghu
W.P.Carey School of Business
Arizona State University
raghu.santanam@asu.edu

Zhan Shi
W.P.Carey School of Business
Arizona State University
zmshi@asu.edu

Abstract

The General Data Protection Regulation (GDRP) is considered a significant step in global privacy laws. Our paper reveals counterintuitive and heterogeneous effects of GDPR on business performance in the digital products market from an international trade perspective. Based on a unique dataset, we empirically examine whether the rollout of the GDPR affects internal and external mobile app performance in European countries by using a difference-in-differences framework. We find that, in European countries, the implementation of GDPR has significantly increased the performance of mobile apps published outside the EU and decreased the performance of mobile apps published within the EU. We further conduct comprehensive robustness checks and explore the mechanisms. This paper reveals that given the more stringent privacy control instituted by GDPR, consumer privacy concerns over foreign products or services largely reduce. European citizens are more open-minded and willing to use foreign digital goods after the rollout of GDPR.

Keywords: GDPR, digital products, privacy decision making, difference-in-differences, global trade

1. Introduction

With the rise of big data and its increased availability and applications, new services, companies, and markets are emerging. Data has become a crucial input in technology-driven innovations, spanning various industries especially the digital products market. Companies are more and more relying on data and bearing benefits for data subjects and data holders. They are eager to utilize data as a valuable asset to monetize customers in a wide range of applications such as personalized recommendations, advertising, and marketing. For example, digital advertising revenue is projected to reach 460 billion U.S. dollars by 2024. The Federal Trade Commission (2016) also reveals several empowering benefits of big data on impoverished communities including increased educational attainment, specialized healthcare for underserved communities, and better access to employment.

At the same time, however, public concerns over privacy security have arisen given several high-profile consumer data breaches and data misuses. In 2014, the Federal Trade Commission reports that data brokers hold a large amount of information on individual consumers. For example, one data broker holding information on 1.4 billion consumer transactions and over 700 billion data elements, and another broker adding more than three billion new data points to its database each month. Another report finds that 91% of iOS apps and 83% of Android apps exhibit at least one risky behavior, such as location tracking and disclosing personal information.[1] The Federal Trade Commission (2016) also highlights further possible risks that could result from data misuse such as more individuals deny potential beneficial opportunities, existing disparities being reinforced, and the

[1] https://www.prnewswire.com/news-releases/appthority-exposes-security-and-privacy-risks-behind-top-400-mobile-apps-245968521.html

URI: https://hdl.handle.net/10125/103161
978-0-9981331-6-4

weakening of consumer choice. A direct result of these scandals is the increasing concerns from consumers- the public producers of the valuable asset. In recent years, the increasing tension between how firms and organizations collect, use and store personal data and individual privacy has reached a tipping point in recent years. A 2018 Pew survey reveals that 91% of respondents have concerns over how personal information is collected and used, 61% would like to take some actions to protect their privacy, and 66% said current regulations are insufficient and believe more laws are needed for protecting their privacy (Rainie 2018). Another survey by McKinsey (2019) on 1000 North American consumers also points out that individual users are becoming more and more cautious about what types of data they share and with whom. With the increasing concerns over privacy security, governments announce new rules (e.g., the General Data Protection) enforcing more stringent requirements on privacy protection, setting new standards.

The GDPR is a privacy and security law drafted and passed by the European Union (EU). It was adopted in EU on April 14, 2016, becoming effective two years later on May 25, 2018. As a result of the regulation that mandates a higher level of privacy, users can access, correct, and erase their personal data. Failure to comply can result in potentially hefty fines, regardless of where the data is processed. There are conflicting reports regarding how GDPR has affected firms and organizations. On one side, the stringent policy incurs high compliance cost and thus forces some companies leave the European market[2]. Some have to give up the products and services that targeting on European citizens[3]. On the other side, some companies find opportunities and adapt to this change by adjusting their business models. The New York Times, for example, switched from behavioral advertising to contextual and geographically targeted ads on its EU site after GDPR and it worked out well[4]. In the literature, researchers also reveal that the impacts of privacy regulation on consumers and firms are heterogeneous. Studies point out that GDPR causes an inhibiting effect on consumer data permissions (Zarsky 2016, John et al. 2011, Gilman and Cooper 2009) and adds administrative and legal compliance costs to the collection of consumers' personal information (Cooper 2012, Campbell et al. 2015, Mello et al. 2018), which in turn has a significant negative impact on firm outcomes (Goldfarb and Tucker 2011, Miller and Tucker 2009, Kim and Wagman 2015). At the same time, there are many studies find that privacy regulations that granting consumers intensified control over their personal information reduce privacy concerns and engender trust among users to increase data allowances (Cavusoglu et al. 2016, Stutzman et al. 2013, Xu et al. 2009, 2012, Brandimarte et al. 2013). The increased data allowances will further enable firms and organizations to make better data strategies and to target more on users who are amendable to data-driven marketing (Godinho and Adjerid 2021). Researchers also show that the impacts can be heterogeneous, depending on the specific attributes of privacy laws and whether it indeed addresses the privacy concerns (Adjerid et al. 2016, Miller and Tucker 2018).

Given the theoretical ambiguity surrounding their impacts, we aim to answer the question with a focus on the digital products market from an international perspective. This paper examines the impacts of GDPR on digital products produced both within and outside the EU markets. We leveraged a quasi-natural experiment setting to quantify the impact of GDPR rollout on mobile app top charts of 155 countries all over the world. We create a unique dataset, which combines daily most popular mobile app lists for multiple countries from 2016 to 2018 and mobile app publisher country information collected manually and automatically. This study utilizes a difference-in-differences (DID) model on the monthly importer - exporter data with both importer countries and exporter countries are divided into two groups (within EU and outside EU). Specifically, we compare the difference in the number of time apps published within EU appear on top chart lists of GDPR countries comparing to that of apps published outside EU before and after GDPR implementation. Our results reveal that after the implementation of GDPR, in the mobile app top chart lists within the EU region, the percent of apps published outside of EU increase significantly and the percent of apps published within EU reduced significantly. We then conduct several additional analyses and robustness checks and find that these patterns still hold. Additionally, we also find evidence on app-country level and the conclusions are consistent. We take a step further and dig into the underlying mechanisms. Specifically, we divide the apps into privacy related categories and non-privacy related categories and check the heterogeneous

[2] https://money.cnn.com/2018/05/25/media/gdpr-news-websites-la-times-tronc/index.html

[3] https://www.trendmicro.com/vinfo/us/security/news/online-privacy/closing-shop-or-closing-off-companies-respond-to-gdpr

[4] https://digiday.com/media/gumgumtest-new-york-times-gdpr-cut-off-ad-exchanges-europe-ad-revenue/

impacts before and after GDPR implementation. We find that the impacts are more salient for apps in privacy-related categories. Before the implementation, EU citizens are more willing to use mobile apps within their region. After the implementation of GDPR, mobile users within the EU become more open-minded given the mandatory protection and are more willing to download and use mobile apps outside EU region. This is counterintuitive since, according to the literature, the pass of free trade agreement usually benefits the contracting parties. Our findings reveal that the regulation actually improves the performance of digital products from countries outside the regulated areas.

Our results have significant implications for individual consumers, firms, organizations, and government regulators. Additionally, there is currently limited work evaluating the impact of GDPR, especially from a global perspective (Libert et al. 2018, Goldberg et al. 2019, Peukert et al. 2020; Jia et al. 2021, Godinho and Adjerid 2021). Considering GDPR's new and drastic changes, the existing body of evidence does not fully reveal of whole picture of its imacts. Taking a global perspective, we evaluate the impacts of privacy regulation on the performance and outcome of businesses in the digital products market (Goldfarb and Tucker 2011, Miller and Tucker 2009, Adjerid et al. 2016, Miller and Tucker 2018). We also add to the literature on consumer privacy decision making (Xu et al. 2009, Smith et al. 2011, Xu et al. 2012, Adjerid et al. 2016). In previous studies, researchers found that transparent communication and increased control over personal information relieve safety concerns, incite trust, and encourage data sharing and disclosures (such as Cavusoglu et al. 2016, Miyazaki and Krishnamurthy 2002, Brandimarte et al. 2013). This paper further demonstrates that the increased trust could help overcome the physical and cultural distance in international trade. We provide evidence on the unintended benefits of data regulation on the non-contracting parties and negative effects on contracting and protected parties because of the consumer decision making change given the mandatory privacy protection. These findings will be useful to policymakers addressing data privacy and security regulations. Regulations and policy makers should consider the unintended benefits and increased competition provided by regional data regulations. The proliferation of data and privacy regulations around the world presents new challenges and new opportunities for organizations. The paper outlines a potential business area worth exploring by international companies.

2. Literature Review

2.1. Implications of data protection and privacy laws

Acquisti et al. (2016) review the growing literature that investigates the implications of data policies and data regulation. Most of the works report negative and harmful effects of data regulation on system efficiency. In healthcare markets, Miller and Tucker (2009, 2011) investigate the effects of a health-related data regulation and find that the adoption of electronic medical records significantly decreased after the launch of privacy laws on publishing patient information. Hoel and Iversen (2002) investigate a related issue about the US states banned the use of genetic information and find that system efficiency significantly reduces when test information changes from private to public. Also, Miller and Tucker (2018) find that giving users more control over disclosure deters individuals from obtaining genetic tests. In financial markets, according to Kim and Wagman (2015), mortgage denial rates decreased significantly when stricter financial-privacy laws were enacted, which may contribute to an increase in foreclosure rates.

There are some studies exploring the impact of privacy and data laws in a similar setting to the GDPR. For example, the ePrivacy Directive, known as ePrivacy in Europe, was implemented in 2002. The 2002 privacy directive negatively impacts funding of smaller EU ventures, as reported by Lambrecht (2017). In response to the directive, smaller firms may have invested disproportionate resources complying with its guidelines or opted not to serve their potential customers, consequently decreasing revenue and growth prospects, thereby reducing investments in those types of ventures.

In 2018, GDPR is implemented as a new attempt made to give EU citizens improved control over their privacy. It is one of the most important changes and strengthening of privacy regulations in decades. Researchers have conducted several works to understand and quantify the impacts of this regulation. For example, Goldberg et al. (2019) provide evidence that for EU firms, after the rollout of GDPR, the web traffic reduces significantly. Jia et al. (2021) report that GDPR reduces on the number of venture deals, especially the ones that are newer, data-related, and consumer-facing ventures in the period immediately following GDPR’s implementation. Aridor et al. (2020) estimate about a decline of 12.5% in trackers adopted by major ad networks in the European travel sector following the rollout of the GDPR. They demonstrate that consent denial harms companies' ability to track users across websites, diminishes the performance of target ads and offers, leading to revenue losses. Peukert et al. (2020) point out that websites reduce the number of third-party web technology providers they use, in particular relating to third-party cookies after the GDPR.

We position our work within this research area on the business impact of the more stringent and mandatory privacy protections provided by data regulations, wherein we study the impact of the GDPR in the digital products market from an international perspective. Through exploring the underlying mechanisms of the patterns revealed in the results, we also draw upon another research stream regarding the behavioral change on the consumer side.

2.2. Privacy decision making

The literature on privacy decision making reveals conflicting patterns on the impacts of improved data control on customer data allowances and disclosure. The key discussion point is about whether more stringent rules increase scarcity and cost associated with data collection or engender trust and alleviate concerns (Miyazaki and Krishnamurthy 2002, Xu et al. 2009, 2012, Smith et al. 2011, Cavusoglu et al. 2016, Brandimarte et al. 2013). One stream of work suggests that granting consumers more flexibilities and controls over personal information would result in a negative effect on consumer data permissions (Zarsky 2016, Cooper 2012, Gilman and Cooper 2009). For example, existing studies highlight the potential of more strict consent requirements to largely reduce the availability of data critical to technology initiatives (Gilman and Cooper 2009, Mello et al. 2018). Further, John et al. (2011) conduct experiments and find that the adoption of transparent privacy notices indicating higher privacy protections can ironically have negative effects on disclosure. Except for making personal information scarcer, data regulations will likely add administrative and legal compliance costs to the collection of consumers' personal data. Many theoretical works (such as Krasteva et al. 2015, Campbell et al. 2015) also point out that data regulation and its engendered compliance costs could generate entry barriers and thus stifle innovation.

On the other hand, some researchers also provide opposite evidence. For example, Cavusoglu et al. (2016) and Stutzman et al. (2013) both reveal that, since Facebook started implementing more detailed privacy settings, data sharing has greatly increased. Godinho and Adjerid (2021) also find that enhanced consumer consent provided by the data regulation increases data disclosure and further increases the performance of targeted marketing of the firms. Granting individuals more controls over their personal data seems to be a particularly efficient way for alleviating privacy concerns and increasing data allowances and disclosure. Following the logic of these works, if consumers are more confident that firms will behave responsibly with their data in light of the regulation (Tikkinen-Piri et al. 2018, Goddard 2017), they could have increased trust over the products or service offering within the region under this regulation. The increased trust and confidence could open their mind to try more products or services they would not to because of security concerns, especially for products or services from a different culture. This expectation motivates the research question of this paper.

3. Data and Methodologies

3.1. Research context

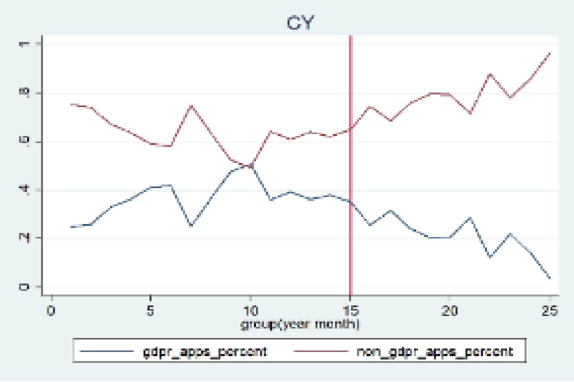
The General Data Protection Regulation (GDPR) was officially implemented in May 2018 in 30 European Union countries. This regulation's goals are to protect customer privacy, standardize data collecting and processing, and prevent data misuse. No matter where they are situated, all businesses and organizations that offer goods or services to EU citizens are required by this rule to give persons control over their personal data. In addition, GDPR requires consent to be able to be updated or withdrawn as easily as it can be granted. GDPR represents a major advance in protecting consumers' privacy. This intensified and regulated protection may lead to a change in the behavior of EU citizens regarding digital products, specifically mobile apps. This in turn may shift the flow of international trade in mobile apps. With this expectation, we delve into an international mobile app usage data and find model free evidence

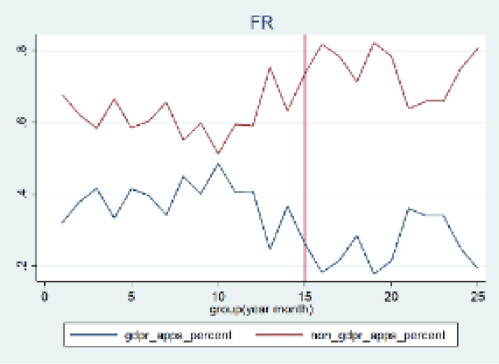
3.2. Data and model-free evidence

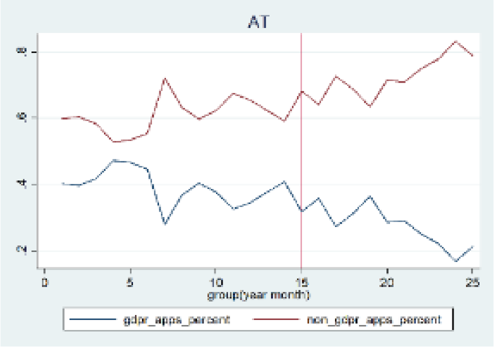
Our primary data is the international mobile app top charts data covering 155 countries over three years. We collected the top 30 chart app list with their ranking information every month from March 3, 2017 to April 30, 2019. Our dataset includes a total of 25,166 distinct apps that appeared on the top chart lists at least once. We then collected the publisher country information for the sampled apps. We first gathered the app publisher information from Sensortower.com, a professional mobile app tracking website. For the apps that we did not find records on the website, we manually searched the publisher country information by checking their developer websites. Through all the ways we could use, there are still 50% of the total apps that we were not able to identify their publisher country.

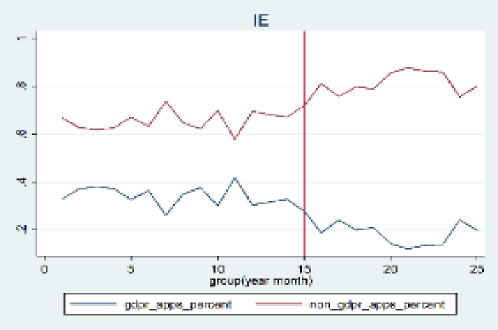
The goal of the study is to investigate the effects of the GDPR on the performance of apps, developed within and outside of EU, in the EU markets. Specifically, we attempt to investigate how the performance of native apps and foreign apps change after the GDPR rollout in EU. Appearing in the top chart and achieving a spot is an indicator of high download and good performance. We operationalize the performance of country i's app in country j as percent of apps on country j's top chart list that are published by country i. We organize the data into country pair level with country i indicates publisher country (exporter) and country j indicates use country (importer). Each country pair has 26 records indicating the 26 months.

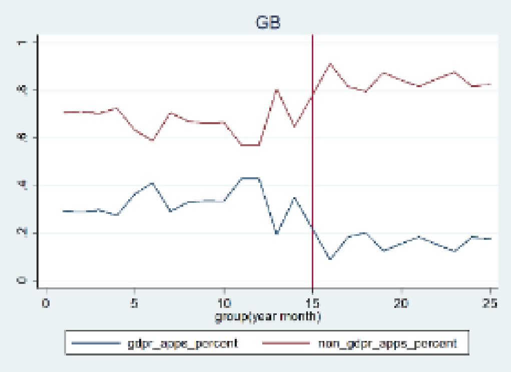
To check whether there are some intuitive patterns, we first explore the data and plot the percent of apps on the top chart list from EU versus outside of EU along the time for several EU countries that are under the protection of GDPR. As shown in Figure 1, there is evidence that trends are similar in 2017 and 2018 (before May). One noticeable feature is the distinct level shift in outcomes in the post-GDPR period. The model-free evidence clearly shows that after the implementation of GDPR, there are more apps from non-GDPR countries appear in those countries' top chart and there are fewer apps from GDPR region that get into the top chart of those countries.

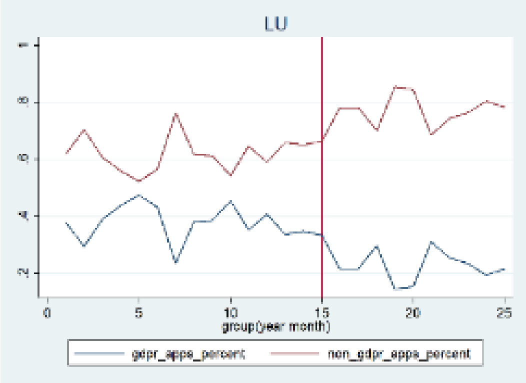












(CY- Cyprus; FR- France; AT- Austria; IE- Ireland; GB- Great Britain; LU - Luxembourg)
X axis represents month, Y axis represents percent of apps in the Top Chart (among apps that we know their publisher country) that from GDPR region (blue line) and from non-GDPR region (red line). The vertical line represents 2018, May when GDPR became enforceable.

Figure 1. GDPR countries' top chart composition.

3.3. Econometric models

To address this research question, we organize the data to import (use country) - export (publisher country) structure on a country-pair-month basis. This data structure design is similar to the one that is widely used in the international trade literature using gravity model (e.g., Dai et al. 2014). Specifically, we have 155*155 country pairs over 26 months. We test the impacts of the GDPR using a difference-indifferences (DID) methodology (Bertrand et al. 2004) and specification is as follows:

$$X_{ijt} = \beta_0 + \beta_1 * GDPR_{ijt} + \beta_2 * GDPR_{noijt} + \rho_{it} + \theta_{jt} + \gamma_{ij} + \epsilon_{ijt} \quad (1)$$

Our dependent variable x_{ijt} is how much percent of country j's top apps (apps appear in the top chart and have publisher information) are from country i at time t. A higher number indicates better performance of mobile apps from a country i in a country j. $GDPR_{ijt}$ indicates whether country i and country j are both within GDPR region at time t. It becomes 1 in post-GDPR periods (after May 2018) if both i and j are covered by GDPR. $GDPR_{noijt}$ is an indicator that takes value 1 if exporter i is not covered by this regulation and importer j is covered by this law in post-GDPR periods (after May 2018). ρ_{it} is a set of time-varying exporter (source/publisher) fixed effects. θ_{jt}. Also, there is a set of time-varying effects for the importer (destination) - θ_{jt}. Finally, γ_{ij} is a set of country-pair fixed effects. In literature investigating how free trade agreements impact internal trade (Baier and Bergstrand 2002), country-pair fixed effects are used to address the endogeneity of free trade agreements.

3.4. Main results

We run the above model and the estimation results are shown as in Table 1 column (1). We find that $GDPR_{ijt}$ has a significant negative effect and $GDPR_{noijt}$ has a significant positive effect. The interpretation is after the rollout of GDPR, there are more apps that are published in courtiers outside of the EU region appear in GDPR countries' top chart lists. At the same time, there are significantly fewer native apps published within the EU region in the top charts. In these results, we consider both internal and external trade, in other words, country i could equal to country j in our dataset. We test the validity of the results based on the sample that excluding internal trade.

Accordingly, we re-estimate the model and the results are shown in Table 1 column (2). We still observe a significant positive effect for $GDPR_{ijt}$ and a significant negative effect for $GDPR_{noijt}$ while using a different sub-sample. In the following session, we conduct several additional analyses and robustness checks to further validate the results.

Table 1. Estimation results of GDPR on EU countries' popular app list compositions.

<table>
<tr><td></td><td>(1)</td><td>(2)</td></tr>
<tr><td>DV</td><td>ln(<i>TopChart%</i>)</td><td>ln(<i>TopChart%</i>)</td></tr>
<tr><td>$GDPR_{ijt}$</td><td>-0.0024***
(0.00)</td><td>-0.0020***
(0.00)</td></tr>
<tr><td>$GDPR_{noijt}$</td><td>0.0005***
(0.00)</td><td>0.0004***
(0.00)</td></tr>
<tr><td colspan="2">Country Pair Fixed Effect</td><td>Included</td></tr>
<tr><td colspan="2">Importer-Year Fixed Effect</td><td>Included</td></tr>
<tr><td colspan="2">Exporter-Year Fixed Effect</td><td>Included</td></tr>
<tr><td colspan="2">Month Fixed Effect</td><td>Included</td></tr>
<tr><td>Sample</td><td>All country pairs</td><td>Only consider external usage</td></tr>
<tr><td>Observations</td><td>721,370</td><td>717,340</td></tr>
<tr><td>R - Squared</td><td>0.969</td><td>0.969</td></tr>
</table>

*** p<0.01, ** p<0.05, * p<0.1. Robust standard errors clustered at Country Pair level in parentheses.

3.5. Robustness checks and additional analysis

3.5.1. Alternative estimator and excluding outliners

For the main results, we use the OLS estimator with the log-transformed dependent variable. Following the literature of gravity model, we also run the Poisson pseudo maximum likelihood (PPML) model suggested by Santos Silva and Tenreyro (2006). The results are shown in Table 2 column (1). The coefficients of the two dummy variables are consistent with our main analysis results. Another confounding factor may be that a large portion of mobile apps consumed in GDPR countries are published in U.S. or China. For the sake of excluding the possibility that what we finding is simply a US or China effect, we re-estimate our model excluding observations involving either the United States or China. This analysis is therefore intended to address the possibility that influential observations are driving the observed relationship. We present the results in Table 2 column (2). We confirm that the results remain unchanged when we exclude the two major countries. Therefore, we conclude that U.S. or Chinese mobile apps are *solely* not driving the observed relationships.

Table 2. Robustness checks results of GDPR on EU countries' popular app list composition.

	(1)	(2)
DV	*TopChart%*	ln(*TopChart%*)
$GDPR_{ijt}$	-0.2629*** (0.028)	-0.00247*** (0.00)
$GDPR_{noijt}$	0.1226*** (0.021)	0.00028*** (0.00)
Country Pair Fixed Effect		Included
Importer-Year Fixed Effect		Included
Exporter-Year Fixed Effect		Included
Month Fixed Effect		Included
Model or Sample	PPML	Excluding US&CN
Observations	721,370	704,106

*** p<0.01, ** p<0.05, * p<0.1. Robust standard errors clustered at Country Pair level in parentheses.

3.5.2. Granular level analysis

All the previous analyses are done at the country pair level. In this session, we use granular level data (i.e., app-country level data) to investigate the impacts of GDPR. We tracked the apps that have appeared in the top charts of 155 countries and constructed a panel data sample for those apps tracking their performance with the EU. The unit of analysis is app-country and the data capture the performance trend of one app in one specific country of the EU. For the dependent variable, we track whether the app has appeared in the top chart list of the specific country at least once for this month, and the number of times an app appears in specific countries' top charts (daily average of the month). We collect the publish dates for all the apps and generate two dummy variables to capture the implementation of GDPR. $GDPR\_Time$ equals 1 if the current date is after May 2018. $GDPR\_Region$ equals 1 if the app's publisher country is within the EU. Through this design, we focus on the apps' performance on the top chart lists of EU countries and divide the apps into groups using dummy variables according to whether the publisher countries belong to the EU. We control for the year fixed effects, month fixed effects, importer country time-variant fixed effects, exporter country year variant fixed effects, country pair fixed effects, app-specific fixed effects, and app category fixed effects. As shown in Table 3, the results in the two columns all present a consistent pattern that the regulation increases the performance for apps within the EU published outside the region and harms the performance of apps within the EU published within the region.

Table 3. Estimation results of the app - country level analysis.

	(1)	(2)
DV	*TopChart*	ln(*Num_TopChart*)
$GDPR\_Time$	0.001*** (0.000)	0.0004*** (0.000)
$GDPR\_Time$ * $GDPR\_Region$	-0.002*** (0.000)	-0.00058*** (0.000)
ln(AppAge)	-0.010*** (0.000)	-0.003*** (0.000)
Year Fixed Effect		Included
Month Fixed Effect		Included
Importer Year Fixed Effect		Included
Exporter Year Fixed Effect		Included
Country Pair Fixed Effect		Included
App Fixed Effect		Included
App Category Fixed Effect		Included
Observations	3,888,240	3,888,240
R-squared	0.339	0.499

*** p<0.01, ** p<0.05, * p<0.1. Robust standard errors clustered at app level in parentheses.

3.5.3. Underlying mechanisms

Through the analyses above, we conclude that GDPR has a significant positive effect on mobile apps published outside of the EU and has a significant negative effect on mobile apps published within the EU. The results are robust and consistent with all the additional analyses. In the next step, we further explore the underlying mechanisms. Following the literature, we expect that the regulation engenders the trust and confidence of the customers in the products or services offered within the region given the mandatory compliance. Thus, the regulation reduces consumers' concerns about privacy, particularly when it comes to foreign products imported from other regions. Therefore, if this expectation is true, we may expect a significant heterogeneity effects of GDPR for different app categories with different privacy sensitivity.

To test this, we divide the app category into two groups: privacy-related categories and non-privacy-related categories (see Table 4), based on anecdotal evidence.

Table 4. The list of privacy related app categories vs. non-privacy related categories.

Non-Privacy Related	**Privacy Related**
Book	Business
Catalogs	Entertainment
Education	Finance
Food & Drink	Games
Reference	Health & Fitness
Magazines & Newspapers	Medical
Utilities	Shopping
Weather	Social Networking
News	Photo & Video
Music	Lifestyle

Accordingly, we partition the sample into two – one only considering apps in privacy-related categories and the other one only considering apps in non-privacy-related categories. We then estimate the same model on the two samples, and the results are presented in Table 5. We find that the effects of GDPR on native apps and foreign apps are significant for apps in privacy-related categories and not significant for apps in non-privacy-related categories, which check our expectations and validate the proposed mechanism.

Table 5. Heterogeneous effects upon privacy.

	(1)	(2)
DV	ln($TopChart\%$ $PrivacyApps$)	ln($TopChart\%$ $NonPrivacyApps$)
$GDPR_{ijt}$	-0.005*** (0.001)	0.0002 (0.000)
$GDPR_{noijt}$	0.0014*** (0.000)	0.0001 (0.000)
Year Fixed Effect		Included
Month Fixed Effect		Included
Importer Year Fixed Effect		Included
Exporter Year Fixed Effect		Included
Country Pair Fixed Effect		Included
Observations	721,370	721,370
R-squared	0.790	0.927

*** p<0.01, ** p<0.05, * p<0.1. Robust standard errors clustered at Country Pair level in parentheses.

4. Conclusions and Implications

While big data has been developing rapidly and is affecting our lives more and more deeply, data and privacy concerns arise among individual users all over the world. In line with this, policymakers have been making efforts to regulate the market and the use of data. To achieve better efficacy, the increasing impacts of data and privacy regulations have to be studied (Goddard 2017; Goldberg et al. 2019). This study explores the impact of the GDPR on the performance of digital products within EU region from an international trade perspective. Specifically, we investigate the performance of mobile apps published within and outside the EU on the top charts of EU countries. We use a unique global mobile app market panel data of most popular mobile app lists each day over 155 countries before and after GDPR implementation. By conducting the DID model, we compare the differences in the percent of EU top chart apps that are published from EU before and after the GDPR rollout against the difference in the percent of EU top chart apps that are published outside EU. In contrast to the negative average effects of GDPR already established by past research, we show evidence of GDPR's unanticipated benefits on international digital products performance. We performed further analyses and robustness checks to validate these results. Our findings are consistent and robust to these extensions. This paper reveals after the rollout of GDPR, EU citizens reduce their privacy concerns over foreign digital products and become more confident and more willing to use products outside their territory given the mandatory protection.

This study adds to the body of knowledge by introducing creative viewpoints and avenues for future investigation. First, this study contributes to the existing literature concerning whether and how GDPR affects consumers and firms (such as Godinho and Adjerid 2021) and the larger extant research stream on data and privacy regulations, with a specific focus in the digital products market from an international perspective. Second, our study also contributes to the literature on privacy decision makings. According to prior studies, stricter data laws can relieve privacy concerns and incite trust (such as Xu et al. 2009). Based on the previous findings, we further demonstrate that the engendered trust and confidence may help reduce home bias and promote long-distance trade. Nowadays, cultural distance and physical distance still matter in the international trade in the digital era, our study points out a potential way to pierce the veil of cultural distance.

Finally, our paper contributes to an ongoing debate in the literature. In the late 1960s, the Internet was created as extra-terrestrial, at once political rebellious and was a borderless realm of spectacular innovation and profit gained through a standardized web architecture. As the number of web users and uses expand and as its importance increases immensely, privacy and security issues arise. Citizens look to the state for their privacy protection. At the same time, the default setting of the state is to attempt to exert territorial control in the digital world. For various economic and political reasons, governments take actions to protect citizens and serve national interests, which incurring the extension of sovereign control. The move towards data localization creates new frictions and barriers in digital trade and can curtail the economic benefits of digital connectivity. There is a raising fear that the balkanization of the Internet will damage the economic potential and slow the innovation and growth. As a result of this fragmentation (what some researchers have called the ‘splinternet’), international digital trade and the global economy would suffer. As the literature on “Splinternet” and “Internet Balkanization” points out (e.g., Azmeh et al. 2020). GDPR is a privacy regulation scenario where “soft” data localization is encouraged through more storage of data within the EU. The findings in our study reveals that GDPR does appear to promote the cross-border/culture digital trade. We identify data and privacy regulation is indeed a win-win for meeting legitimate concerns and promoting digital trade and the prospects for innovation and growth the global digital economy. Organizations and firms can make better decisions in this rapidly evolving and highly competitive global environment when they know the costs and benefits of data and privacy regulations.

5. References

Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. Journal of Economic Literature, 54(2), 442-92.

Adjerid, I., Acquisti, A., Telang, R., Padman, R., & Adler-Milstein, J. (2016). The impact of privacy regulation and technology incentives: The case of health information exchanges. Management Science, 62(4), 1042-1063.

Aridor, G., Che, Y.K., & Salz, T. (2020). The economic consequences of data privacy regulation: Empirical evidence from GDPR (No. w26900). National Bureau of Economic Research.

Azmeh, S., Foster, C., & Echavarri, J. (2020). The international trade regime and the quest for free digital trade. International Studies Review, 22(3), 671-692.

Baier, S.L., & Bergstrand, J.H. (2002). On the endogeneity of international trade flows and free trade agreements. New York: mimeo.

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced confidences: Privacy and the control paradox. Social Psychological &Personality Science, 4(3), 340-347.

Campbell, J., Goldfarb, A., & Tucker, C. (2015). Privacy regulation and market structure. Journal of Economics & Management Strategy, 24(1), 47-73.

Cavusoglu, H., Phan, T.Q., Cavusoglu, H., & Airoldi, E.M. (2016). Assessing the impact of granular privacy controls on content sharing and disclosure on Facebook. Information Systems Research, 27(4), 848-879.

Cooper, J.C. (2012). Privacy and antitrust: Underpants gnomes, the first amendment, and subjectivity. The Geogre Mason Law Review, 20, 1129.

Dai, M., Yotov, Y.V., & Zylkin, T. (2014). On the trade-diversion effects of free trade agreements. Economics Letters, 122(2), 321-325.

Federal Trade Commission. (2014). Data brokers: A call for transparency and accountability. https://www.ftc.gov/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014.

Federal Trade Commission. (2016). Big data: A tool for inclusion or exclusion? https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf.

Gilman, D.J., & Cooper, J.C. (2009). There is a time to keep silent and a time to speak, the hard part is knowing which is which: striking the balance between privacy protection and the flow of health care information. Michigan Telecommunications & Technology Law Review, 16, 279.

Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. International Journal of Market Research, 59(6), 703-705.

Godinho de Matos, M., & Adjerid, I. (2021). Consumer consent and firm targeting after GDPR: The case of a large telecom provider. Management Science. ePub ahead of print September 8, https://doi.org/10.1287/mnsc.2021.4054.

Goldberg, S., Johnson, G., & Shriver, S. (2019). Regulating privacy online: The early impact of the GDPR on european web traffic & e-commerce outcomes. Available at SSRN 3421731.

Goldfarb, A., & Tucker, C.E. (2011). Privacy regulation and online advertising. Management science, 57(1), 57-71.

Hoel, M., & Iversen, T. (2002). Genetic testing when there is a mix of compulsory and voluntary health insurance. Journal of Health Economics, 21(2), 253-270.

Jia, J., Jin, G.Z., & Wagman, L. (2021). The short-run effects of the general data protection regulation on technology venture investment. Marketing Science, 40(4), 661-684.

John, L.K., Acquisti, A., & Loewenstein, G. (2011). Strangers on a plane: Context-dependent willingness to divulge sensitive information. Journal of consumer research, 37(5), 858-873.

Kim, J.H., & Wagman, L. (2015). Screening incentives and privacy protection in financial markets: A theoretical and empirical analysis. The RAND Journal of Economics, 46(1), 1-22.

Krasteva, S., Sharma, P., & Wagman, L. (2015). The 80/20 rule: Corporate support for innovation by employees. International Journal of Industrial Organization, 38, 32-43.

Lambrecht, A. (2017). E-Privacy Provisions and Venture Capital Investments in the EU. Working paper, London Business School, London, United Kingdom.

Libert, T., Graves, L., & Nielsen, R.K. (2018). Changes in third-party content on European News Websites after GDPR. Report, Reuters Institute for the Study of Journalism, Oxford, UK.

McKinsey & Company (2020) The consumer-data opportunity and the privacy imperative. Report, McKinsey & Company, worldwide.

Mello, M.M., ADLER-MILSTEIN, J.U.L.I.A., Ding, K.L., & Savage, L. (2018). Legal barriers to the growth of health information exchange—boulders or pebbles? The Milbank Quarterly, 96(1), 110-143.

Miller, A.R., & Tucker, C. (2009). Privacy protection and technology diffusion: The case of electronic medical records. Management Science, 55(7), 1077-1093.

Miller, A.R., & Tucker, C. (2018). Privacy protection, personalized medicine, and genetic testing. Management Science, 64(10), 4648-4668.

Miller, A.R., & Tucker, C.E. (2011). Can health care information technology save babies? Journal of Political Economy, 119(2), 289-324.

Miyazaki, A.D., & Krishnamurthy, S. (2002). Internet seals of approval: Effects on online privacy policies and consumer perceptions. Journal of Consumer Affairs, 36(1), 28-49.

Peukert, C., Bechtold, S., Batikas, M., & Kretschmer, T. (2020). European privacy law and global markets for data. Available at SSRN 3560392.

Rainie, L. (2018) Americans' complicated feelings about social media in an era of privacy concerns. Accessed on August 10, 2020. http://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/.

Silva, J.S., & Tenreyro, S. (2006). The log of gravity. The Review of Economics & statistics, 88(4), 641-658.

Smith, H.J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. MIS Quarterly, 989-1015.

Stutzman, F.D., Gross, R., & Acquisti, A. (2013). Silent listeners: The evolution of privacy and disclosure on Facebook. Journal of privacy and confidentiality, 4(2), 2.

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: changes and implications for personal data collecting companies. Computer Law & Security Review, 34(1), 134-153.

Xu, H., Teo, H.H., Tan, B.C., & Agarwal, R. (2009). The role of push-pull technology in privacy calculus: the case of industry self-regulation, and government regulation on privacy concerns: a study of location-based services. Information Systems Research, 23(4), 1342-1363.

Xu, H., Teo, H.H., Tan, B.C., & Agarwal, R. (2012). Research note—effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: a study of location-based services. Information Systems Research. 23(4), 1342-1363.

Zarsky, T.Z. (2016). Incompatible: the GDPR in the age of big data. Seton Hall Law Review, 47, 995.