Short Run Effects of Generalized Data Protection Act on Returns from AI Acquisitions

Rajkumar Venkatesan
Ronald Trzcinski Professor of Business Administration
University of Virginia
Darden Graduate School of Business, Charlottesville, VA 22903
E-Mail: Venkatesanr@darden.virginia.edu

S. Arunachalam
Assistant Professor of Marketing
Indian School of Business, India
E-mail: s_arunachalam@isb.edu

Kiran Pedada
Assistant Professor of Marketing
Indian School of Business, India
E-mail: kiran_pedada@isb.edu

Short Run Effects of Generalized Data Protection Act on Returns from AI Acquisitions

Abstract

The General Data Protection Regulation (GDPR), enacted in 2016, provides guidelines to firms on using personal customer information and empowers customers to know the ways firms use their data. We study the effect of GDPR on return on assets from acquisitions of AI technology companies. The objective of AI acquisitions matters after GDPR. Though firms obtain positive returns from AI acquisitions after GDPR, returns are low and weakly significant. However, returns are higher after GDPR for AI acquisitions that improve customer experience and cybersecurity. Returns from AI acquisitions to improve efficiency and product innovations are unchanged after GDPR. Revenue improvements and cost reductions from AI acquisitions are unaffected after GDPR. Our study documents AI acquisition strategies that can benefit firms after GDPR.

Short Run Effects of Generalized Data Protection Act on Returns from AI Acquisitions

Introduction

Governments institute privacy regulations, such as GDPR and CCPA, to improve customer welfare. The regulations require firms to ask consumers' consent to use their data in AI algorithms and empowers consumers to ask firms to either delete their data or show the ways their data is used by firms. GDPR and CCPA also restrict firm's ability to share consumer information to other firms like third party data aggregators without explicit consent. The regulation themselves are a response to the widespread use of personal consumer information by firms to target consumers. Recognizing this tradeoff between privacy and economic performance, scholars have called for research that explores factors that can allow firms to use AI algorithms effectively in the presence of privacy regulations (Varian 2019, Martin and Palmatier 2020).

AI helps firms create and deliver superior customer value (Insaniti and Lakhani 2020) through personalized products and services (Venkatesan and Lecinski 2021). In terms of creating customer value, AI can help firms improve customer experience and develop innovative products. Ulta Beauty invested in AI technology to offer augmented reality and virtual try ons for hair color, makeup and eyebrow shaping on their mobile apps. IntelligentX, a UK based brewing company's AI algorithms use customer feedback about beer preferences to provide suggestions about new brew recipes to the brew master. In terms of delivering value, AI allows firms to streamline their processes to improve efficiencies, and secure customer information. For example, chatbots can improve efficiency and cost of customer service by providing responses to routine questions and directing only complex queries to humans. AI can help firms develop better cybersecurity protocols that monitor and detect data breaches. Expectation of higher

returns from personalization is driving firms across industries to increase their investment in developing AI capabilities (The CMO survey 2021). These AI algorithms use personal consumer information to identify their preferences and design personalized solutions. Hence, the growth of AI based solutions has also coincided with rise in privacy concerns among consumers and regulators. More than 50% of consumers surveyed by McKinsey and the Pew Research center are concerned about the privacy of their emails, downloaded files, location data, and the content and usage of online chat rooms[1].

But do privacy regulations curtail firms' ability to create and deliver customer value using AI? Anecdotal and research evidence suggests that firm are directing resources away from AI initiatives under privacy regulations (Bessen et al. 2020, Jia et al. 2021). The industry reports cite one reason for this decline is expectations that, under privacy regulations, the AI algorithms would have less accurate predictions and hence firms would obtain lower returns from AI investments[2]. GDPR poses restrictions on firms' ability to used personalized customer data that is a critical input for AI technologies. The accuracy of AI algorithms could hence be lower if firms use aggregate or market level information because customers do not provide consent to use individual level information.

However, findings in the privacy literature suggests that privacy regulations may affect the returns from certain types of AI investments more than the others. The concept of privacy paradox states that even though consumers express privacy concerns in surveys, they do not take actions to protect their privacy and data (Aquisiti 2004). Research on consumer behavior in the presence of GDPR also provides mixed results. While the number of visitors to a website reduces

[1] https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative
[2] https://iapp.org/news/a/want-europe-to-have-the-best-ai-reform-the-gdpr/

after GDPR, the number of pages visited by the customer in fact increases (Goldberg et al. 2021). Consumers also have less privacy concerns when they perceive higher control of their data. All this suggests that firms may be able to obtain consumer consent even under privacy regulations and subsequently be able to provide superior value using AI.

It is therefore not obvious if the returns from AI investments in value creation and delivery that use historic, granular information about customers would in fact be lower under privacy regulations. Firms and policy makers would hence be interested in knowing the effect GDPR has on the returns that firms can obtain from AI technology acquisitions. In this research, we explore the value firms can obtain from AI investments when there are privacy regulations. In addition, we estimate the heterogeneity in returns across different strategic objectives of AI investments.

We focus on firms that build AI capability through acquisitions in this research. Firms can develop technology capabilities either by building them in-house or by acquiring technology firms with AI capabilities[3]. Acquisitions of AI firms grew by more than 280% from 2016 to 2019[4]. Acquisitions are an attractive option for growth because firms can obtain skills and capabilities at a faster rate through acquisitions than the alternative of building capabilities inhouse[5]. Further, the investments of firms in acquisition of AI technology are clearly identified from announcements of acquisitions by publicly traded firms. On the other hand, firms' investments to build AI technology capabilities in-house cannot be identified easily from company filings. We therefore aim to address the following research questions:

- *What is the effect of GDPR on returns from AI acquisitions?*

[3] https://www.bcg.com/publications/2018/build-buy-dilemma-artificial-intelligence
[4] https://www.ciodive.com/news/AI-acquisitions-mergers-ipo-ma-2019/570964/
[5] https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/the-six-types-of-successful-acquisitions

- *What AI acquisition objectives; value creation (customer experience, innovation), and value delivery (cybersecurity, operational efficiencies), provide higher or lower returns in the presence of GDPR?*

We assemble a rich dataset from multiple sources to empirically test our research propositions. We used the Factiva database to identify the list of AI-related acquisition announcements made by the US and European firms between the years 2010 and 2019. We supplemented this data by the COMPUSTAT annual financial data. The final sample consists of 289 AI-related announcements made by US and European firms between 2010 and 2019.

Our research replicates findings from prior research on the effect of GDPR on the customer level (Goldberg et al. 2021) to the firm level. Consistent with existing research on acquisition performance (Meyer-Doyle et al. 2019), we use the return on assets (ROA) of firms as the dependent variable. On average, GDPR exposure reduces the ROA of firms. We also find that GDPR exposure increases the ROA of firms that make AI acquisitions for improving customer experience, and cybersecurity. Returns on AI investments in innovation and operational efficiencies are unaffected by GDPR.

Our study contributes to the emerging literature on customer privacy and AI marketing strategy. We show that contrary to conventional wisdom, privacy regulations in fact improve returns from investment in AI capabilities. We also identify AI investment areas, i.e., customer experience, and cybersecurity, that provide the highest returns in the presence of AI regulations. Our results show that ROA of firms that acquired AI firms with a customer experience objective increased by 15.46 percent points after GDPR and by 23.44 percent points for firms that acquire AI firms with a cybersecurity objective. Our research can help direct firms' efforts in building

their AI capability in the presence of privacy regulations. The results from our research can also help regulators promote the benefits of their regulations to industry organizations.

Next, we present the conceptual background and our expected effects. Later we explain the data collection process and the empirical model used to test the hypotheses. We then present the results of our analyses and derive the managerial and theoretical implications of our research. We conclude with the limitations of our research and identify venues for future research.

Conceptual Background

According to the Resource Based Theory (RBT), firms' bundles of resources provide them a competitive advantage (Barney 1991). Eisenhardt and Martin (2000) extend RBT to propose that in dynamic market environments firms need to also dynamically update their capabilities to match the changing competitive conditions and consumer preferences. AI and machine learning algorithms are a bundle of resources that provide firms the capabilities to improve value creation and delivery (Isantini and Lakhani 2020). Further, consumer familiarity with technology, market regulations and the technology of AI is constantly evolving. Hence the resource based theory and the closely related dynamic capabilities theory is an appropriate theoretical framework for our research.

Benefits from using AI algorithms. The literature provides evidence for considering AI as a bundle of resources that can provide competitive advantage. Firms find value from data analytics that is used to process and develop innovations by combining a diverse set of existing technologies (Wu et al. 2020)[6]. Data driven decision making and predictive analytics provided manufacturing firms productivity gains between 2005 and 2015 (Brynjolfsson and McElheran 2019). Performance gains from predictive analytics (including AI and machine learning) is

[6] Research on the value of data analytics for firms is relevant to our research because AI technologies are built on data analytics.

higher for firms that also invest in complementary capabilities including efficient production practices, and employee education (Bynjolfosson et al. 2021). Firm AI investments, measured as hiring of AI skilled workers, results in higher sales growth, and improvements in market share especially for ex-ante larger firms (Babina et al. 2020). Further, firms see gains from AI investments in product innovation (including personalization) and geographic expansion more than process improvements.

We classify a firms' AI activities into two buckets, (a) value creation, and (b) value delivery similar to Insaniti and Lakhani (2020). AI acquisitions that improve value include acquisitions focused on customer experience and innovation. We define *AI Customer Experience* as the use of AI and machine learning to enhance customer value creation including customer insights, customer buying experience, personalization of product and service offerings, and customer support. Firms can use AI to leverage historic data on customer interactions to enhance the experience in future transactions for all customers. For example, Spotify used AI to enhance listeners experiences by providing options such as hand-picked songs, personal playlists, and virtual radio stations. Similarly, Netflix learns from the historical data to tailor movie recommendations and improve live streaming.

AI algorithms used to improve customer experience exhibit positive network effects. AI algorithms improve over time in better understanding customer preferences as a firm collects more data about existing and new consumers. The value provided by a firm increases over time due to the increasing quality of consumer insights from AI algorithms.

Literature on personalization has focused on customer targeting and display advertisements. Rossi et al. (1996) shows that firms can gain profits from targeting customers for discounts using their purchase history data. Venkatesan and Farris (2012) show that retailers can

improve customer profits by targeting coupons that match customer preferences. Effectiveness of contextual, static and small ads decrease in the presence of privacy regulations, but the effectiveness of contextual, large and dynamic ads is unchanged (Goldfarb and Tucker 2011b). Display advertisements that are both obtrusive and targeted perform worse than advertisements that are either obtrusive or targeted (Goldfarb and Tucker 2011a).

Personalized and customized customer experiences are expected to improve customer loyalty and engagement (Lemon and Verhoef 2016). Firms that can track customers across channels and provide an omnichannel, personalized customer experience can improve retention and customer profitability. Personalized recommendation systems have a positive effect on sales (Pathak et al. 2014). Personalized emails which include the recipient's name have higher open rates and lead to more sales even when they are non-informative (Sahni et al. 2018).

Value Delivery. Cybersecurity and operational efficiency are the two aspects of value delivery enhanced by AI technologies. AI Cybersecurity technologies enable firms to protect private customer information and monitor security threats. This improves the quality of service delivery and improves customer trust (Awuah Peprah et al. 2021).

Information security (or cybersecurity) technologies use AI algorithms to detect and monitor data breaches and cyberattacks. These technologies use information from previous attacks to detect patterns and use machine learning to detect anomalies in network activities. These AI algorithms help firms reduce the possibility of data breaches though enhanced encryption of data on consumer facing apps and prediction of data breach events. We define, *AI Cybersecurity* as the investments in monitoring and detection of security breaches to enhance protection and privacy of customer and firm data.

Literature on customer consequences of data breaches is relatively nascent compared to the rich literature in information systems on the business consequences and stock market reactions to information security and cybersecurity. Since privacy regulations is about responsible usage of customer data, we focus our attention on the literature relevant to customer reactions to cybersecurity threats and data breaches.

Customer spending reduces following a data breach and this effect is lower for customers with higher prior spending (Janakiraman et al. 2018). Customers of a matchmaking site showed reduced search and messaging activity on the site following a data breach (Turjeman and Feinberg 2019). Acquisitions of cybersecurity firms happen irrespective of a data breach incident. The research on customer and stock market reactions to data breach incidents provide justification for firm investments in technology that avoids data breaches. There is however scarce research on consumer reactions and firm performance consequences to investments in cybersecurity technology.

We define, *AI Operational Efficiency* as the use of AI and machine learning to reduce costs, improve the efficiency of workflows, and reduce manufacturing risks and defects. Firms use AI to improve the internal workflow and improve operational efficiencies. For example, the Indian telecom company, Airtel leverages AI to improve operational efficiency by automatically identifying and resolving network issues and managing network capability in real-time. Babina et al (2020) document that AI investments in process improvement do not influence firm performance. AI investments in process improvements may however have an indirect influence on consumer value. They enable firms to deliver consumer value (Iansiti and Lakhani 2020) effectively and efficiently. Investments in process improvements rely on data from firm activities more than consumer transactions with the firm. Often, algorithms used to improve internal firm

processes mask or encrypt the identity of consumers. Process improvements allow firms to justify their product or service's prices and improve consumer loyalty by providing a consistent and flawless experience.

Consumer Data Privacy Regulations. Wide usage of individual consumer information has raised concerns about data privacy among consumers and policy makers. These widespread concerns about data privacy led to the institution of privacy and data use regulations in Europe, GDPR, and in California, CCPA. The objectives of the privacy regulations are to protect consumers and encourage responsible usage of consumer data by firms.

The privacy regulations, such as GDPR, restrict firms from using consumer data without their direct consent. They ensure firms use consumer data only for the activities that consumers provide consent to firms. This prevents sale of consumer data to third party aggregators and the use of aggregated consumer information to target consumers with ads or product offers. These regulations also restrict the history of data firms can store. Firms need to provide consumers, upon request, a record of firm activities that used the consumers' data. Consumers also have the right to request firms to delete their data.

Tradeoffs with privacy regulations. Firms and consumers face important tradeoffs with privacy regulations. Consumer data is necessary to provide enhanced value. But the regulations restrict the firms to use consumer data only for activities that they have explicit consumer consent. Evidence on the effects of privacy regulations on firm performance is mixed (Acquisiti et al. 2016). Anecdotal evidence and early evidence from academic literature (Campbell et al. 2015) suggests that large firms benefit from privacy regulations because they can absorb the costs of complying with regulations. Privacy paradox suggests that consumers are more willing to share private information with companies even if they state concerns about privacy in surveys

(Acquisiti 2004). Several empirical studies provide evidence of this paradox. Majority of consumers do not opt-out of targeted ads that use personalized data. In a field experiment that evaluated the Adchoice program, Johnson et al. (2020) find that less than 1% of advertisements served to consumers were opt-out ads after the implementation of the program. The opt-out ads generated 58% less revenue than comparable ads that were targeted. These results are striking when contrasted with majority of consumers expressing privacy concerns in surveys. One explanation for the privacy paradox is that consumers experience less privacy concerns and are willing to transact more with firms when they feel in control of their data (Martin et al. 2017).

Practitioners predicted that GDPR will slow investments in AI capabilities[7]. However, empirical evidence in the academic literature on the effects of GDPR are mixed. Schmitt et al. (2021) demonstrate consequences of GDPR on user behavior across several websites. Among websites that experienced a reduction in total users visiting the website, the number of visits per user in fact increased, after GDPR. The drop in number of user visits is higher for smaller websites than larger websites. Visits to business and consumer service websites increased after GDPR. In contrast, Goldberg et al. (2021) show that recorded page impressions from EU users decrease after GDPR. A study on the effects of the GDPR on technology venture investment revels that investments in European startups have dropped by about 36% compared to the US and other global startup since the introduction of GDPR (Jia et al. 2021). However the financial effects of firm investments in AI algorithms in the presence of privacy regulations is less understood.

Developing firms' AI capabilities. Firms develop capabilities either in house or through acquisition of firms with the desired capabilities. Firms can obtain complimentary assets using

[7] https://www2.datainnovation.org/2018-impact-gdpr-ai.pdf

acquisitions when the technology uncertainty is declining (Moeen and Mitchell 2020). Moreover, when compared to other modes of governance, acquisitions present better control over the acquired AI capabilities and offer better coordination and alignment of complementary resources across value chain activities (Dyer and Singh 1998; Taylor and Helfat 2009). Therefore, firms tend to use acquisitions over other governance modes to gain access to specialized resources such as AI capabilities (Hartmann and Henkel 2020; Moeen and Mitchell 2020). In this paper, we focus on firms building AI capability through acquisitions.

We do not consider the factors studied in previous research including exploration, exploitation, financial slack, and complementarity in knowledge (e.g., Makri, Hitt, and Lane 2010) because of the context of the current study. Since we use an exogenous shock, i.e., GDPR exposure, we consider that all the other factors are similar before and after the shock.

Our research explores the moderating role of privacy regulations on the effect of firm AI acquisitions (customer experience, innovation, cybersecurity, and operational efficiency) on financial performance. Based on prior research (e.g., Son et al. 2014; Steelman et al. 2019) we expect a positive main effect of acquisitions, and AI capabilities on financial performance. We contribute to the existing literature by exploring the moderating role of privacy regulations on the financial outcomes from AI acquisitions in this research.

Value Creation

Firm investments that enhance consumer value and experience provide positive returns (Sorescu and Sorescu 2016). AI capabilities can help firms deliver personalized experiences and develop new products that fit consumer preferences. Privacy regulations restrict firms from using customer data for any activities without their consent. These regulations prevent firms from sharing information freely with third party vendors without consumer consent. Firms hence need

to obtain information directly from consumers, i.e., first party data, instead of using information provided by third party data aggregators. Consumers are also likely to provide firms consent for activities that directly enhance value rather than selling customer data to other data aggregators or for using information from data aggregators to promote the firms' products.

AI acquisitions for improving customer experience and product innovation allow firms to rely on first party consumer data. Without in house AI capabilities, firms need to share consumer data with third party vendors to deliver improved customer experience and develop innovative products. Consumers have lower privacy concerns when their information is stored locally on their mobile phones than transmitted to a central server (Sutanto et al. 2013). This would imply that consumers would have lower privacy concerns when their information is stored within a firm and not shared with third party vendors.

Privacy regulations can increase consumers' perception of control over their personally identifiable information because they force companies to be transparent about their data collection practices. Firms on the other hand benefit from providing experience value in addition to mere economic value in exchange for personal information (Martin et al. 2020). Consumers are likely to favor entrenched firms and are less likely to try new firms in the presence of strong opt-in requirements of a privacy regulation (Campbell et a. 2015). Consumers have a positive reaction to targeted and personalized advertisements when their perception of control of their personally identifiable information is higher (Tucker 2014, Xu et al. 2012). The negative effects of privacy concerns are reduced with firms' transparency and consumer control of the firms' data management practices (Martin et al 2017). In contrast, consumers' difficulty in assessing the collection, use and protection, of their data negatively affects their willingness to download a mobile app (Al Natour et al. 2020).

These findings suggest that loyalty and trust among consumers would be higher for firms that use AI investments to improve customer value especially when the issues of data privacy are salient in the market. We therefore expect that privacy regulations enhance the positive effect of customer experience and innovation focused AI acquisitions on firm performance.

Value Delivery

Firms that invest in cybersecurity can gain customer trust especially in markets with privacy regulations. Consumers will see firms investing in AI technologies for cybersecurity as acquiring state of the art technologies to protect their personal information. Consumers are more likely to purchase from firms that better protect their information especially when privacy issues are salient (Tsai et al. 2011). While firms are in general not adequately equipped for cybersecurity (Jain et al. 2018), consumers would view their investments in cybersecurity favorably. In a lab experiment, Athey et al. (2017) show that consumers are more likely to trust firms and less likely to use technologies that prevent firms from tracking customers, when they are provided information about privacy protections. This leads us to predict that customers would react more positively to firm investments in cybersecurity technology especially in the presence of privacy regulations. We therefore expect that privacy regulations enhance the positive effect of cybersecurity focused AI acquisitions on firm performance.

We treat AI acquisitions for operational efficiency as a placebo test. Privacy regulations focus on the responsible usage of consumer data. AI acquisitions for reducing costs and improving the efficiency of the workflow do not depend on consumer data. We therefore do not expect privacy regulations to moderate the effect of operational efficiency on firm performance. We summarize our expectations in Table 1.

Table 1: Summary of Expectations

Variable	Expected Effect	Brief Rationale
Customer Experience	+	AI acquisitions for improving customer experience and innovation allow firms to rely on first party consumer data. Furthermore, privacy regulations can increase consumers' perception of control over their personally identifiable information leading to increased consumer loyalty and trust.
Innovation	+	
Cybersecurity	+	Consumers perceive cybersecurity focused AI investments as acquiring state of the art technologies to protect their personal information. Moreover, consumers are more likely to trust firms when they are provided information about privacy protections.
Operational Efficiency	NA	We do not expect an effect of operational efficiency because AI acquisitions for improving operational efficiency of the workflow do not depend on consumer personal information.

NA – Not Applicable

Short Run Effects of Generalized Data Protection Act on Returns from AI Acquisitions

Data Collection

We assemble our dataset from multiple sources. First, we used the Factiva database to identify the list of AI-related acquisition announcements made by US and European firms between the years 2010 and 2019. To identify the AI-related acquisitions, we created a set of keywords based on the literature on business applications of AI (Garbuio and Lin 2019). Our list of keywords includes "*artificial intelligence", "AI" "robotics", "robotic process automation", "RPA", "machine learning", "deep learning", "neural network", "autonomous", "chatbot", "virtual agent", "digital assistant", "natural language processing", "NLP" and "computer vision".* Once, we identified the AI-related acquisition announcements, we used the COMPUSTAT database to collect the financial data of the firms in the dataset. The final sample consists of 289

AI-related announcements made by US and European firms from 2010 to 2019.

Natural Language Processing of the Announcements

We analyzed the AI-related acquisition announcements using topic modeling to discover both the topics prevalent in AI acquisition announcements and the words that comprise these topics. We use the latent Dirichlet allocation (LDA) method of topic modeling to simultaneously extract a set of keywords found in the AI acquisition annoucements, and the clustering of the keywords into latent topics or themes of AI acquisition objectives. Topic models assume that documents have one or more latent topics that generate the observed words or keywords. Further, the latent topics can be identified by the greater than random co-occurrence or clustering of certain keywords within the latent topics. Prior literature has used LDA for topic modeling to analyze innovation announcements (e.g., Dotzel and Shankar 2019) and social media posts (e.g., Tirunillai and Tellis 2014).

Table 2: Classification of the Acquisition Objectives and Keywords from Topic Modeling

Customer Experience	**Innovation**	**Cybersecurity**	**Operational Efficiency**
customer engagement, client support, client value, client satisfaction, customer enhancement, customer understanding, customer analytics, help clients, personalized solutions, customer experience, customer service, customized offering, customer information, customer benefits, customer value, user experience, customer convenience, customer support, automation	innovation, technology enhancement, product portfolio, new product development, product and services development, technology, R&D, intellectual property, product expansion, product transformation	Customer protection, customer information, monitoring, cybersecurity, inspection, security, privacy, safety, protection, threat protection, threat detection, malware protection	Lower cost, flaw detection, efficiency, risk reduction, cost saving, operational efficiency, detection, cost effective, operating cost, process efficiency, speed, streamline operations, defect recognition,

As part of a rigorous implementation of LDA, we removed "stop" words and "connecting" words (e.g., and, but, if), some common words in most announcements (e.g., company, group), and company names. Four topic clusters, customer experience, innovation, cybersecurity, and operational efficiency, emerged from the LDA analysis. The identified topics are in line with the AI activities classification provided in existing literature (Insaniti and Lakhani 2020). The keywords comprising these topics are provided in Table 2.

Following the recommendation of Berger et al. (2020) to combine human judgement with topic modeling, two independent coders carefully read through the purpose of the announcements and classified them into 4 categories – customer experience, security, operational efficiency, and innovation using keywords identified in Table 2. The intercoder reliability using proportion reduction in the loss method was .95, above the threshold (.8) recommended by Krippendorff (2013). This process ensured coders other than the researchers, with limited domain knowledge and without the bias of the researchers, classified the documents using keywords provided by the LDA and in the process also verified the classification quality provided by the LDA (Rinke et al. 2021).

Variable Operationalization

Dependent Variable

The dependent variable for this study is ROA. We use ROA as the measure of firm performance because it has been used extensively in the marketing literature to measure firm performance (e.g., Feng, Morgan, and Rego 2015; Rust et al.2004; Srinivasan and Hanssens 2009). ROA is computed as the ratio of the firm's income before extraordinary items to the firm's total assets. We calculate ROA using financial-accounting data a year after the acquisition announcement ($ROA_{(t+1)}$).

Focal Independent Variables

GDPR exposure is a dummy variable that equals 1 if either the acquirer or the target firm is part of the EU and the time of acquisition is after May 2018 (i.e., post the enactment of GDPR) and 0 otherwise. Our operationalization recognizes that a firm is exposed to GDPR rules if any part of its organization has operations in Europe, either if the firm is the target or the source of the acquisition.

Customer experience is a dummy variable that takes the value of 1 if the motivation of the AI-related acquisition is related to improving customer experience and 0 if this reason is not mentioned. *Innovation* is a dummy variable that takes the value of 1 if the motivation of the AI-related acquisition is related to innovation and 0 if this reason is not mentioned. *Cybersecurity* is a dummy variable that takes the value of 1 if the motivation of the AI-related acquisition is related to improving cybersecurity and 0 if this reason is not mentioned. *Operational efficiency* is a dummy variable that takes the value of 1 if the motivation of the AI-related acquisition is related to enhancing operational efficiency and 0 if this reason is not mentioned.

Table 3 provides the correlation table of the model variables and their descriptive statistics. The table shows a shows positive correlation of GDPR, and all four AI acquisition objectives with ROA. The correlation among the independent variables is low, suggesting multicollinearity is not likely an issue in our analyses. About 30% of the firms in our sample have GDPR exposure.

Table 3: Descriptive statistics and correlations Among Variables

	1	2	3	4	5	6	7	8	9
1 ROA	1								
2 GDPR Exposure	0.091	1							
3 Customer Experience	0.008	-0.203	1						
4 Innovation	0.032	-0.208	0.038	1					
5 Cybersecurity	0.178	0.032	-0.025	0.035	1				
6 Operational Efficiency	0.025	-0.010	-0.019	-0.055	-0.073	1			
7 SG & A Expenses	0.002	-0.026	0.058	-0.029	0.075	0.007	1		
8 R&D Expenses	-0.006	-0.004	0.041	-0.035	0.091	-0.096	0.509	1	
9 Total Assets	0.100	-0.167	-0.060	0.026	-0.141	0.091	-0.054	-0.065	1
Mean	0.042	0.318	0.519	0.771	0.104	0.609	49.950	8.925	61,457.32
Standard Deviation	.2425	0.467	0.501	0.421	0.306	0.484	523.708	77.077	108,049.3

Notes. N = 255

Table 4 provides the number of acquisitions before after enactment of GDPR by the type of acquisition motivations. Contrary to Jia et al. (2021) who document a decline in venture investment in technology firms, we find that acquisitions of AI firms related to innovation, operational efficiency, and cybersecurity increased post-GDPR. Majority of the AI acquisitions were related to innovation, followed by operational efficiency. These results are also validated by the means for customer experience, innovation, cybersecurity, and operational efficiency reported in Table 3. Acquisition of AI firms for improving customer experience decreased slightly post-GDPR.

Table 4: Number of acquisitions before and after GDPR

Time-period	Customer Experience	Innovation	Cybersecurity	Operational Efficiency
Before GDPR (April 2010 – April 2016)	76	102	12	67
After GDPR (May 2016 – July 2020)	74	121	18	109

Model Specification

The primary objective of our model is to assess (a) the effects of GDPR on return on assets (ROA) of firms that acquire other AI technology firms, and (b) assess the variation in the effect of GDPR across the four acquisition objectives, noted above. Following recent work (Jia et al. 2021) that investigates the casual effects of EU's GDPR, we compare the returns from AI-acquisition of firms exposed to GDPR with those that are not, before and after the enactment of GDPR. We calculate ROA a year after the firm made an AI acquisition. Our specification is:

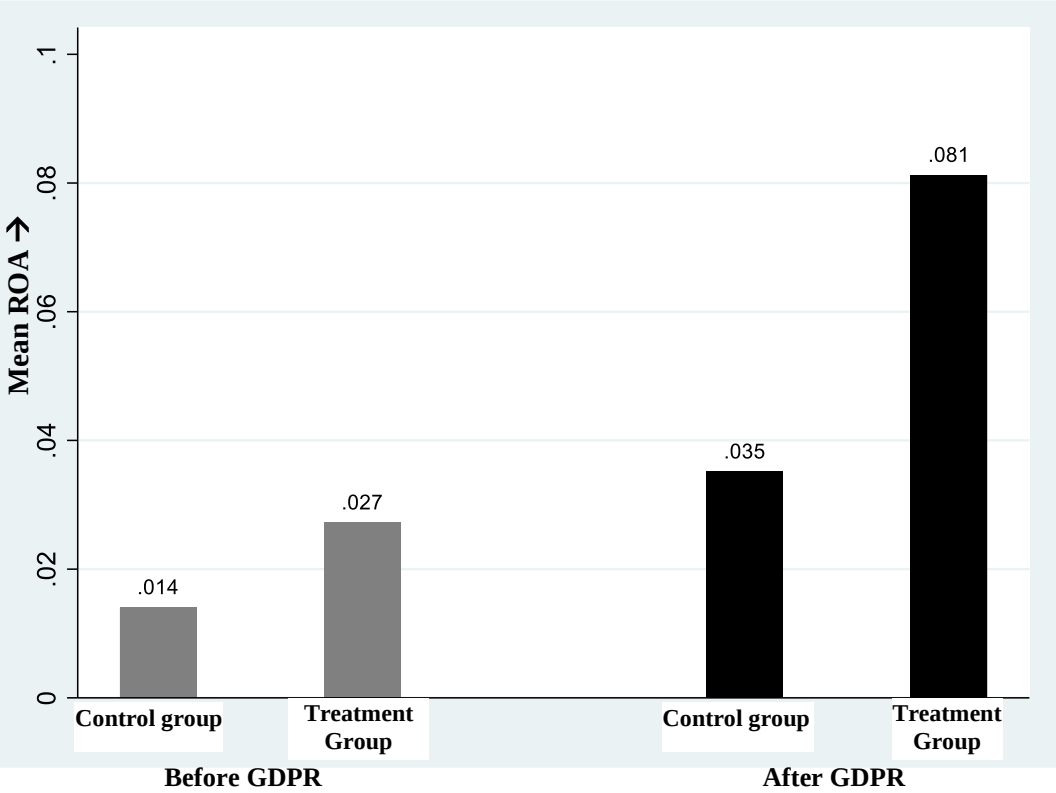
$$ROA_{it+1} = \beta_0 + \beta_1 * GDPR_Exposure_{it} + \beta_2 * Customer\ experience_{it} + \beta_3 * Innovation_{it} + \beta_4 * Cybersecurity_{it} + \beta_5 * Operational\ efficiency_{it} + \beta_6 * (GDPR_Exposure * Customer\ experience)_{it} + \beta_7 * (GDPR_Exposure * Innovation)_{it} + \beta_8 * (GDPR_Exposure * Cybersecurity)_{it} + \beta_9 * (GDPR_Exposure * Operational\ efficiency)_{it} + \beta_{10} * (SG\ \&\ A\ expense_{it}/Total\ Assets_{it}) + \beta_{11} * (R\&D\ expense_{it}/Total\ Assets_{it}) + \beta_{12} * Total\ assets_{it} + e_{it} \quad (1)$$

where, i and t are subscripts for firm and year respectively.

ROA is the Return on Assets of the acquirer from one year post the year of acquisition (t), GDPR_Exposure is a dummy variable that equals 1 if either the acquirer or the target firm is part of the EU and the time of acquisition is post May 2016 (i.e., post the GDPR) and 0 otherwise, and variables customer experience, innovation, cybersecurity, and operational efficiency are the four-acquisition objectives dummy variables. In equation 1, the parameters of interest are β_6 - β_9, that capture how GDPR moderates the effect of four types of AI acquisitions

on ROA. Finally, the control variables are sales, general and marketing (SG&A) expenses, research and development (R&D) expenses and total assets. These are firm-specific variables of the acquirer firm that could possibly correlate with that firm's ROA. As detailed in the next section, before estimation, we augment this specification with non-parametric matching to achieve balance between the treatment (i.e., acquirer firms exposed to GDPR) and the control (i.e., acquirer firms not exposed to GDPR) firms, through common empirical support. Recent literature on casual identification of models for timeseries cross sectional data (Imai and Kim 2019, 2021), suggest non-parametric matching as a better alternative to the traditional models with two-way fixed effects.

Figure 1: Model free evidence



Notes: Control group (coded 0) = Acquirer firms not exposed to the GDPR law; Treatment group (coded 1) = Acquirer firms exposed to the GDPR law. The plots are the mean values of ROA in the Y-Axis.

Estimation.

Model Free Evidence. We present model free descriptive evidence before presenting the estimation results to establish the face validity of our results. Figure 1 provides the ROA for treatment and control firms, before and after the GDPR. In the pre-GDPR time, the difference in average ROA of the treatment and control firms (-.013) is not statistically significant. There appears a higher difference in average ROA between treatment and control post GDPR (-.046), but the difference is still not statistically significant. ROA increases by about 5 percent points after GDPR among treatment firms but increases only by about 2 percent points after GDPR among control firms. This suggests a positive directional effect of GDPR on ROA of firms acquiring AI capabilities. Our model results would check the validity of these unconditional means after controlling for firm specific factors. Further, the model free evidence present average effects and our model tests heterogeneity of these effects across AI acquisition objectives.

Matching. It is plausible that the acquisitions in the control group are not a representative comparison (i.e., counterfactual) for the acquisitions in the treatment group. To reduce the ex-ante differences between the two groups and to balance them on observable characteristics we use Coarsened Exact Matching (CEM). Causal claims made from CEM matched data are stronger because of the homogeneity in the treatment and control groups of the analyses sample. CEM (Iacus, King, & Porro, 2011) help us assemble an analyses sample that has a similar distribution of control variables in the treatment and control groups. This helps to ensure that the treatment is the only difference between the treatment and control groups. The firm level covariates used for coarsening were R&D spending divided by total assets, SG&A expenses divided by total assets, and total assets. R&D and SG&A are the two major expense categories at

the firm level and are good proxies for deployment of firm level strategies (Moorman, Du, and Mela 2005). Total assets is a robust measure of firm size. Hence, our intuition is that once we balance the treatment and control on key firm level variables that could have a differential impact on the outcome, our results are robust to any firm-specific differences across the two groups.

Table 5: CEM matching on SGA, R&D, and Total assets

R&D over Total Assets		**Without matching**		**With CEM matching**	
		Before GDPR	***After GDPR***	***Before***	***After***
Control group	Mean	.31	22.44	.35	3.21
	SD*	1.86	134.83	2.01	22.35
	N	67	70	67	67
Treatment group	Mean	.71	8.50	.713	2.47
	SD	3.82	55.40	3.82	16.44
	N	41	77	41	76

SG & A over Total Assets		**Without matching**		**With CEM matching**	
		Before	***After***	***Before***	***After***
Control group	Mean	.80	147.92	.90	8.67
	SD	3.58	979.64	3.86	58.22
	N	67	70	67	67
Treatment group	Mean	1.75	29.32	1.75	9.40
	SD	8.54	180.66	8.54	45.91
	N	41	77	41	76

Total Assets		Without matching		With CEM matching	
		Before	***After***	***Before***	***After***
Control group	Mean	64,232.65	93,718.80	42,681.54	46,031.06
	SD	79,969.31	161,167.97	61,025.82	84,093.76
	N	69	71	69	68
Treatment group	Mean	52,650.81	35,903.16	52,650.81	34,508.07
	SD	727,34.14	76,020.67	72,734.14	75,022.80
	N	41	83	41	81

* SD = Standard Deviation

Table 5 provides the mean and standard deviation of the variables used in the matching procedure for both the groups across two periods. For example, when comparing the mean (SD) values of R&D without matching, we note that they are 22.44 (134.83) for the control group and 8.50 (55.40) for the treatment group in the post GDPR time period. This shows that the average value and the spread of the data on the R&D variable is heterogeneous or non-comparable across the two groups. After CEM matching, we note that the values are 3.213 (22.352) for the control group and 2.471 (16.443) for the treatment group. This shows that in the matched sample, the means and SD across two groups are similar or comparable across the two groups. The multivariate L1 statistic quantifies the overall imbalance of the sample such that perfect balance is indicated by L1 = 0 and larger values indicate larger imbalance between the treatment and the control groups. L1 statistic decreased from .2027 in the unmatched sample to .1159 in the matched sample. Subsequently we used the matched sample to test the hypothesized relationships. The matching process reduced the observations from 289 to 284, and in the next step of estimation, missing values in (ROA, marketing expenses, R&D expenses, and total assets) reduced the final analyses sample to 248 observations.

We used STATA's 'CEM' command to run this procedure. The output of CEM command in STATA, automatically generates weights for each observation stored in a variable named '*cem_weights'*. These weights are used to conduct a weighted OLS estimation of equation

1. Following recommendations by the developers of CEM algorithm (Blackwell, Iacus, King, and Porro, 2009), we include the covariates used in the matching process in equation 1 to control for any remaining differences after the matching process.

TABLE 6: Model Estimates

	ROA	ROA
GDPR exposure	0.070†	-0.148*
	(0.037)	(0.085)
Acquisition motivations		
Customer experience	0.026	-0.030
	(0.032)	(0.037)
Innovation	0.029	-0.016
	(0.040)	(0.051)
Cybersecurity	0.152***	0.005
	(0.054)	(0.065)
Operational Efficiency	0.031	-0.011
	(0.032)	(0.038)
SG&A expenses/Total assets	0.000	0.000
	(0.000)	(0.000)
R&D expenses/Total assets	-0.000	-0.000
	(0.001)	(0.001)
Total assets	0.000†	0.000**
	(0.000)	(0.000)
GDPR exposure *customer experience		0.158**
		(0.069)
GDPR exposure *innovation		0.074
		(0.078)
GDPR exposure *cybersecurity		0.366***
		(0.111)
GDPR exposure *operational efficiency		0.099
		(0.068)
Intercept	-0.059	0.047
	(0.050)	(0.062)
N	248	248
R-square	.0605	.1725

Notes. Both the models included CEM matching. Standard errors in parentheses.
† $p < 0.10$ * $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Model Estimates. Table 6 provides the results of estimating equation 1 with and without the interaction terms. From the main effects model, it is seen that that the effect of GDPR on ROA of firms exposed to the law is positive and significant (.070, $p < .05$). The interaction

effects model shows that the moderating effects of GDPR on AI acquisitions with customer experience objectives (.158, $p < .001$) and cybersecurity objectives (.366, $p < .001$) are positive and significant. The main effect of GDPR on ROA, after controlling for the interactions with AI acquisition objectives is negative and significant (-.148, p<.05). This suggests that firms that do not invest in customer experience and cybersecurity through AI acquisitions have a lower ROA post GDPR.

Figure 2A: Effect of GDPR on ROA of firms with customer focused AI acquisitions

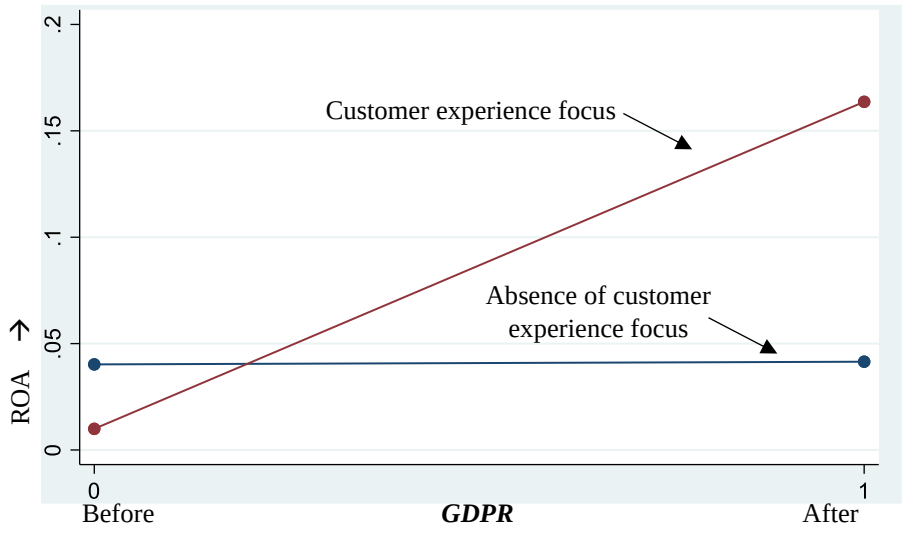
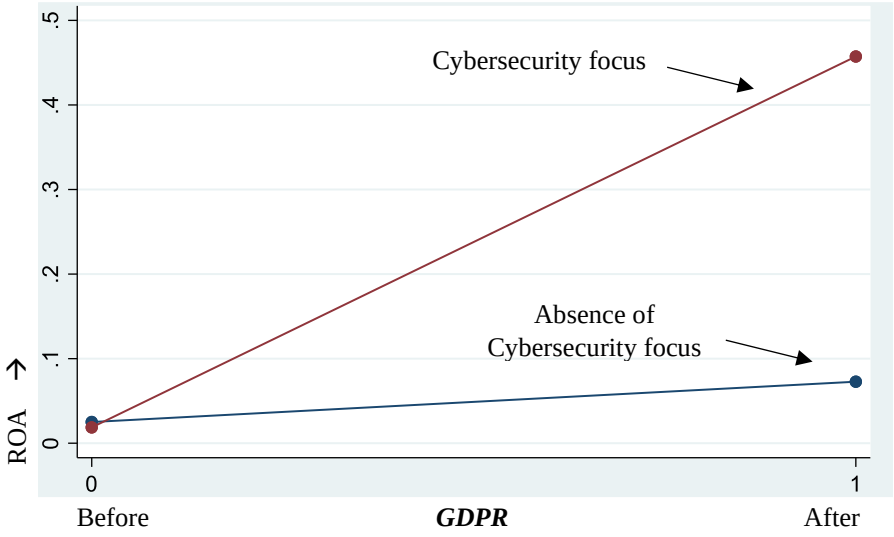


Figure 2B: Effect of GDPR on ROA of firms with cybersecurity focused AI acquisitions



The marginal plots in Figure 2 elaborate on the moderating effect of GDPR on returns from AI acquisitions. ROA increases after GDPR at a much higher rate for firms that make AI acquisitions focused on customer-experience and cybersecurity This supports our arguments that GDPR could benefit AI acquisitions that had intentions of improving customer engagement and experience and strengthening cybersecurity aspects through AI.

Robustness Checks

We rerun the analysis after controlling for lagged performance to control for unobserved firm specific effects. As shown in Table 7, the results are almost identical to our primary model results. Next, we estimated the model with a different measure of firm performance, namely Tobin's q. Unlike ROA, Tobin's q is a forward looking, accounting-based approximation of market valuation of the acquirer firm in the long-term. Recently studies have shown this metric's theoretical and empirical limitations as the metric undervalues firm's intangible assets like customer and marketing related variables (Bendle and Butt 2018). Given that in our study, we focus on key marketing related motivations in the AI acquisitions, and that Tobin's q is a long-term market valuation metric, we do not expect any impact for the short time-period post the enactment of GDPR. Nevertheless, we re-estimated for the matched sample with Tobin's q as the dependent variable. None of the interaction terms with GDPR exposure had significant effect on Tobin's q.

Table 7: Robustness Check with Lagged performance

Variables	ROA_{t+1} (*SE*)
GDPR exposure	-0.132† *(0.078)*
Acquisition motivations	
Customer experience	-0.022 *(0.034)*
Innovation	-0.004 *(0.047)*
Cybersecurity	0.002 *(0.061)*
Operational Efficiency	-0.003 *(0.035)*
GDPR exposure *customer experience	0.142* *(0.064)*
GDPR exposure *innovation	0.049 *(0.072)*
GDPR exposure *cybersecurity	0.382****(0.103)*
GDPR exposure *operational efficiency	0.081 *(0.063)*
SG&A expenses/Total assets	0.000 *(0.002)*
R&D expenses/Total assets	0.000 *(0.006)*
Total assets	0.000^{+}*(0.000)*
ROA_{it}	0.256****(0.077)*
Intercept	0.028 *(0.056)*
N	248
R-square	.1725

Notes. Models included CEM matching. Standard errors in parentheses;
$^{\dagger}p < 0.10$, $^{*}p < 0.05$, $^{**}p < 0.01$, $^{***}p < 0.001$

Placebo Test. We ran two types of placebo tests to strengthen the robustness of our study's results (shown in Tables 8 and 9 respectively). First, we changed the dependent variable to an unrelated or 'fake' outcome by using '*cost of goods sold* (COGS)'. When regressing the natural lag of COGS on the predictor variables as per our original model, none of the four interaction terms were statistically significant. That is GDPR exposure's interaction with 1.) security (estimate (*SE*) = 1.221 (*1.155*); p = .292), 2.) efficiency (.172 (*.677*); p = .799), 3.) innovation (.577 *(.778*); p = .456), and 4.) customer (1.28 (*.689*), p = .065) were insignificant as it is atheoretical to argue for any relationship between these predictors and COGS due to GDPR.

Table 8: Robustness Check with COGS as dependent variable

Placebo DV = COGS	
GDPR Exposure	-1.136 (0.833)
Acquisition motivations:	
Customer experience	-0.548 (0.373)
Innovation	-0.739 (0.502)
cybersecurity	-0.606 (0.708)
Operational Efficiency	-0.073 (0.38)
GDPR Exposure * Customer experience	1.281† (0.69)
GDPR Exposure * Innovation	0.577 (0.774)
GDPR Exposure * Cybersecurity	1.221 (1.155)
GDPR Exposure * Operational Efficiency	0.173 (0.678)
SG&A expenses/Total assets	0.087*** (0.022)
R&D expenses/Total assets	-0.219*** (0.058)
Total assets	0.000*** (0.000)
Intercept	7.809 (0.599)
N = 251	
R-square = .303	

Notes. Models included CEM matching. Standard errors in parentheses;
† $p < 0.10$, * $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

The second placebo test was conducted using a 'fake' treatment variable, i.e., a randomly generated value of 0 or 1 for the predictor GDPR exposure, and a 'fake' exposure date coded as 1, for all records before the year 2014 and 0 otherwise. When regressing ROA on the interaction of this newly created 'fake' exposure variable with the four predictors, none of the effects were significant and moreover the signs of these effects were negative for customer, security and efficiency.

Table 9: Robustness check with placebo exposure

DV = ROA	Estimate (SE)
Placebo Exposure	-0.011 (0.088)
Acquisition motivations:	
Customer experience	0.025 (0.04)
Innovation	-0.014 (0.05)
Cybersecurity	0.199** (0.064)
Operational Efficiency	0.031 (0.041)
Placebo Exposure * Customer experience	-0.038 (0.065)
Placebo Exposure * Innovation	0.057 (0.078)
Placebo Exposure * Cybersecurity	-0.165 (0.148)
Placebo Exposure * Operational Efficiency	-0.006 (0.067)
SG&A expenses/Total assets	0.000 (0.002)
R&D expenses/Total assets	-0.001 (0.006)
Total assets	0.00† (0.000)
Intercept	-0.017 (0.055)
N = 251	
R-square = .059	

Notes. Models included CEM matching. Standard errors in parentheses;
† $p < 0.10$, * $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$.

Discussion

Consequences of privacy regulations on the returns from AI investments in the presence of privacy regulations is poorly understood. We investigate the changes in returns from AI acquisitions for firms exposed to GDPR using a uniquely compiled dataset of AI acquisitions made by U.S. and European firms between the years 2010 and 2019. On average, ROA is lower for firms with GDPR exposure that make AI acquisitions. However, we also find that ROA of firms with GDPR exposure is higher if they make AI acquisitions that are focused on improving customer experience and cybersecurity. These findings provide important implications for research and practice.

Theoretical Implications

To the best of our knowledge, this is the first study to investigate the returns to AI investments in the presence of privacy regulations. By doing so, we contribute to the emerging literature on customer privacy and AI marketing strategy (e.g., Jia et al. 2021; Puntoni et al. 2021).

Extant research on privacy primarily focused on granular consumer behavior (e.g., Acqusiti et al. 2016; Johnson et al. 2020; Xu et al. 2012). These studies suggest that perceived control over privacy increases a consumer's propensity to click online ads (Tucker 2014). In addition to affecting consumer behavior, privacy regulations can affect the profitability of a firm's strategy to build their AI capabilities (Cui et al. 2021). Our study extends extant research on privacy by investigating the effect of privacy regulation on ROA of firms making AI investments. We show that returns for firms making AI acquisitions related to customer experience and cybersecurity is higher after the rollout of GDPR. This is possible if consumers have a higher sense of control and security of their data after privacy regulations. Trust with institutions and the availability of

explicit channels to address their concerns about transactions with firms increases the volume of transactions in online marketplaces (Pavlou and Gefen 2004). Consumers are also willing to provide personal information and engage with firms if they see the firms prioritizing the security of this information. Privacy regulations make data security and protection salient among consumers. Our study confirms these expectations by showing that firms can obtain higher returns from their AI investments in cybersecurity in the presence of privacy regulations.

Further, our study contributes to the emerging literature on AI in marketing (Puntioni et al. 2021). Firms can leverage AI technologies to provide personalized offerings to their consumers. At the same time, these AI technologies leverage personal data about consumers that raise concerns about privacy, security, and the unintended consequences of data sharing among firms. Extant research does not offer guidance on the tradeoff between value creation through personalized offerings and consumer concerns about privacy (Luo et al. 2021). Our study shows that privacy regulations can in fact help firms resolve the value creation and privacy tradeoff. We show that contrary to conventional wisdom, ROA for firms making investments in AI capabilities around customer experience and cybersecurity is higher in the presence of privacy regulations. This also implies that AI investments that are directed directly towards provide better customer experience can lead to higher returns as long as consumers have institutional assurances about the usage of their data and consumers feel in control of their personal data. In a similar vein, firms can improve consumer trust through their investments in capabilities that improve the security of consumer data, i.e., through AI investments in cybersecurity. Our research hence emphasizes that firms should consider mechanisms to develop trust among consumers when implementing AI strategies in their marketing.

Managerial Implications

Developments in AI technology has provided firms an opportunity to personalize their marketing with the expectation of delivering superior customer experience (Venkatesan and Lecinski 2021). The promise of AI technology is however counterbalanced by consumer privacy concerns related to sharing personal information with firms. Regulators have responded to consumer concerns by enacting privacy regulations. Our research provides strategies for effectively building AI capability in the presence of privacy regulations. We suggest that managers should carefully evaluate the objectives of the AI acquisitions in environments that are exposed to privacy regulations. We show that privacy regulations help firms that are customer focused and protect the customers' personal information. Our results show that when ROA of firms that acquired AI firms with a customer experience objective increased by 15.46 percent points after GDPR and by 23.44 percent points for firms that acquire AI firms with a cybersecurity objective. These values are directly derived from the margin plots shown in Figures 2A & 2B. For instance, post GDPR, ROA margin for firms with a customer experience (cybersecurity) objective, jumped to .164 (0.46), from a pre-GDPR, ROA margin of .01 (0.02) leading to 15.46 (23.44) percent point increase, as reported above.

Although privacy regulations such as GDPR provide benefits to consumers by giving control of their data, firms might perceive these privacy regulations as a financial burden with potential negative consequences[8]. Therefore, firms are cautious about AI investments in environments that are exposed to privacy regulations (Jia et al. 2021). Our research provides evidence that regulations which protect consumer privacy can also benefit firms. We show that regulations can improve trust between firms and consumers. Firms that use AI technology to protect consumer

[8] https://www.dickinson-wright.com/news-alerts/the-gdpr-and-mergers-and-acquisitions

data and deliver personalized value can in fact obtain higher returns when there are regulations which assure consumers of mechanisms to address their privacy concerns. Our research suggests that the decrease in AI investments following GDPR (Jia et al. 2021) may be myopic. Regulators can emphasize to the venture capital industry the better financial outcomes of privacy regulations for AI acquisitions focusing on consumer experience and cybersecurity.

Limitations and Future Research

Our study has limitations that can be foundations for future research. We present firm level effects of returns from AI acquisitions. Our expected effects are based on theories of consumer privacy preferences and trust with institutions and firms. Future research can complement our study by empirically exploring the mechanisms behind our results through lab experiments and granular analyses of the firm objectives for the AI acquisitions. Such analyses will provide more nuanced guidance for both firms and regulators. Future research can also explore the effect of privacy regulations on returns from AI acquisitions on longer term metrics such as customer satisfaction, brand equity and customer lifetime value.

We focus our analyses on firms in the US and Europe. The privacy regulations and consumer expectations vary across the globe. Comparisons of returns from AI acquisitions across developed and developing economies will provide guidance for global AI strategies. AI capabilities can be built in-house and through acquisitions. Future research should contrast the returns from building AI capabilities in-house and through acquisitions in the presence of privacy regimes.

Our study contrasts the effects of AI acquisitions before and after GDPR. The California Consumer Protection Act (CCPA) allows for a contrast of AI acquisitions in the presence of US based privacy regulations. As GDPR and CCPA affect different consumers, comparing these

regulations can help build theories about consumer privacy preferences in Europe and the US. The rollout of privacy regulations across the US states also provides a natural experiment to evaluate consumer privacy preferences across political ideologies, and digital divides.

Conclusion

Firms are challenged to identify strategies for effectively developing customer relationships in the presence of privacy regulations. The enactment of GDPR provides a natural experiment to help estimate the casual effect of regulations on the efficacy of AI technologies that leverage personalized data from consumers. We show that ROA of firms making AI acquisitions is lower after GDPR. The ROA of firms making AI acquisitions in the customer experience and cybersecurity contexts are however higher after GDPR. This shows that, contrary to conventional wisdom, privacy regulations can be helpful for firms. We propose that privacy regulations have the potential for improving consumer trust with institutions and firms which can help firms deliver personalized services to customers.

References

Acquisiti, Alessandro (2004), "Privacy and security of personal information", *Economics of Information Security*, 179-186.

Acquisiti, Alessandro., Curtis Taylor, and Liad Wagman (2016), "The Economics of Privacy," *Journal of Economic Literature*, 52(2), 1-64.

Al-Natour, Sameh, Hasan Cavusoglu, Izak Benbasat, and Usman Aleem (2020), "An Empirical Investigation of the Antecedents and Consequences of Privacy Uncertainty in the Context of Mobile Apps", *Information Systems Research*, 31(4), 1037-1063.

Athey, Susan, Christian Catalini, and Catherine Tucker (2017), "The Digital Privacy Paradox: Small Money, Small Costs, Small Talk", Working Paper 23488

Babina, Tania, Anastassia Fedyk, Alex He, and James Hodson (2020), "Artificial Intelligence, Firm Growth, and Industry Concentration," first draft.

Barney, Jay (1991), "Firm Resources and Sustained Competitive Advantage", *Journal of Management*, 17(1), 99-120.

Bendle, N. T., & Butt, M. N. (2018). The misuse of accounting-based approximations of Tobin'sq in a world of market-based assets. *Marketing Science*, *37*(3), 484-504.

Berger, J., Humphreys, A., Ludwig, S., Moe, W. W., Netzer, O., & Schweidel, D. A. (2020). Uniting the tribes: Using text for marketing insight. *Journal of Marketing*, *84*(1), 1-25.

Bessen, James, Stephen Michael Impink, Lydia Reichensperger, and Robert Seamans(2020), "GDPR and the Importance of Data to AI Startups," *NYU Stern School of Business*.

Blackwell, M., Iacus, S., King, G., & Porro, G. (2009). cem: Coarsened exact matching in Stata. *The Stata Journal*, *9*(4), 524-546.

Brynjolfsson, Erik, Daniel Rock, and Chad Syverson (2021), "The Productivity J-Curve: How Intangibles Complement General Purpose Technologies", *American Economic Journal: Macroeconomics*, 13(1), 333-372.

Brynjolfsson, Erik, and Kristina McElheran (2019), "Data in Action: Data-Driven Decision Making and Predictive Analytics in U.S. Manufacturing", Rotman School of Management Working Paper No. 3422397, 1-49.

Campbell, James, Avi Goldfarb, Catherine Tucker (2015), "Privacy Regulation and Market Structure", *Journal of Economics & Management Strategy*, 24(1), 47-73.

Cui, T. H., Ghose, A., Halaburda, H., Iyengar, R., Pauwels, K., Sriram, S., ... & Venkataraman, S. (2021). Informational challenges in omnichannel marketing: remedies and future research. *Journal of Marketing*, *85*(1), 103-120.

Dotzel, T., & Shankar, V. (2019). The relative effects of business-to-business (vs. business-to-consumer) service innovations on firm value and firm risk: An empirical analysis. *Journal of Marketing*, *83*(5), 133-152.

Dyer, J. H., & Singh, H. (1998). The relational view: Cooperative strategy and sources of interorganizational competitive advantage. *Academy of management review*, *23*(4), 660-679.

Eisenhardt, Kathleen M., and Jeffrey A. Martin (2000), "Dynamic Capabilities: What Are They?", *Strategic Management Journal*, 21(10), 1105-1121.

Feng, H., Morgan, N. A., & Rego, L. L. (2015). Marketing department power and firm performance. *Journal of Marketing*, *79*(5), 1-20.

Garbuio, M., & Lin, N. (2019). Artificial intelligence as a growth engine for health care startups: Emerging business models. *California Management Review*, *61*(2), 59-83.

Goldfarb, Avi, and Catherine E. Tucker (2011a), "Privacy regulation and online advertising", *Management Science*, 57(1), 57–71.

Goldfarb, Avi, and Catherine E. Tucker (2011b), "Search engine advertising: Channel substitution when pricing ads to context.", *Management Science*, 57(3), 458–470.

Goldberg, Samuel, Garrett Johnson, and Scott Shriver (2021), "Regulating privacy online: An economic evaluation of the GDPR," Marketing Science Institute Working Paper Series, Report No. 21-110.

Hartmann, P., & Henkel, J. (2020). The rise of corporate science in AI: Data as a strategic resource. *Academy of Management Discoveries*, *6*(3), 359-381.

Iacus, S. M., King, G., & Porro, G. (2012). Causal inference without balance checking: Coarsened exact matching. *Political analysis*, *20*(1), 1-24.

Iansiti, Marco, and Karim R. Lakhani (2020), "Competing in the Age of AI How machine intelligence changes the rules of business", *Harvard Business Review*, 98(1), 60-67.

Imai, K., & Kim, I. S. (2019). When should we use unit fixed effects regression models for causal inference with longitudinal data?. *American Journal of Political Science*, *63*(2), 467-490.

Imai, K., & Kim, I. S. (2021). On the use of two-way fixed effects regression models for causal inference with panel data. *Political Analysis*, *29*(3), 405-415.

Jain, S. C., & Ropple, L. M. (2018). Stopping Data Breaches Will Require Help from Governments. Harvard Business Review Digital Articles, 1–5.

Janakiraman, Ramkumar, Joon Ho Lim, and Rishika Rishika (2018), "The Effect of a Data Breach Announcement on Customer Behavior: Evidence from a Multichannel Retailer", *Journal of Marketing*, 82 (March), 85-105

Jia, J., Jin, G. Z., & Wagman, L. (2021). The Short-Run Effects of the General Data Protection Regulation on Technology Venture Investment. *Marketing Science*.

Johnson, G. A., Shriver, S. K., & Du, S. (2020). Consumer privacy choice in online advertising: Who opts out and at what cost to industry?. *Marketing Science*, *39*(1), 33-51.

Krippendorff, K. (2013). Commentary: A dissenting view on so-called paradoxes of reliability coefficients. *Annals of the International Communication Association*, *36*(1), 481-499.

Lemon, Katherine N., and Peter C. Verhoef (2016), "Understanding Customer Experience Throughout the Customer Journey", *Journal of Marketing*, 80 (November), 69-96.

Luo, X., Qin, M. S., Fang, Z., & Qu, Z. (2021). Artificial Intelligence Coaches for Sales Agents: Caveats and Solutions. *Journal of Marketing*, *85*(2), 14-32.

Makri, M., Hitt, M. A., & Lane, P. J. (2010). Complementary technologies, knowledge relatedness, and invention outcomes in high technology mergers and acquisitions. *Strategic management journal*, *31*(6), 602-628.

Martin, Kelly D., Abhishek Borah, and Robert W. Palmatier (2017), "Data Privacy: Effects on Customer and Firm Performance", *Journal of Marketing*, 81(1), 36-58.

Martin, Kelly D., and Robert W. Palmatier (2020), "Data Privacy in Retail: Navigating Tensions and Directing Future Research", *Journal of Retailing*, 96 (4), 449-457.

Meyer-Doyle, P., Lee, S., & Helfat, C. E. (2019). Disentangling the microfoundations of acquisition behavior and performance. *Strategic Management Journal*, *40*(11), 1733-1756.

Moeen, Mahka, Will Mitchell (2020), "How do pre-entrants to the industry incubation stage choose between alliances and acquisitions for technical capabilities and specialized complementary assets?", *Strategic Management Journal*, 41, 1450-1489.

Moorman, C., Du, R., & Mela, C. F. (2005). The effect of standardized information on firm survival and marketing strategies. *Marketing Science*, *24*(2), 263-274.

Pathak, Bhavik, Robert Garfinkel, Ram D. Gopal, Rajkumar Venkatesan, and Fang Yin (2014), "Empirical Analysis of the Impact of Recommender Systems on Sales", *Journal of Management Information Systems*, 27(2), 159-188.

Peprah, A. A., Giachetti, C., Larsen, M. M., & Rajwani, T. S. (2021). How Business Models Evolve in Weak Institutional Environments: The Case of Jumia, the Amazon. Com of Africa. *Organization Science*.

Pavlou, P. A., & Gefen, D. (2004). Building effective online marketplaces with institution-based trust. *Information systems research*, *15*(1), 37-59.

Puntoni, S., Reczek, R. W., Giesler, M., & Botti, S. (2021). Consumers and artificial intelligence: An experiential perspective. *Journal of Marketing*, *85*(1), 131-151.

Rinke, Eike Mark, Timo Dobbrick, Charlotte Löb, Cäcilia Zirn, and Hartmut Wessler. "Expert-Informed Topic Models for Document Set Discovery." *Communication Methods and Measures* (2021): 1-20.

Rossi, Peter E., Robert E. McCulloch, and Greg M. Allenby (1996), "The Value of Purchase History Data in Target Marketing", *Marketing Science*, *15*(4), 321-340.

Rust, R. T., Lemon, K. N., & Zeithaml, V. A. (2004). Return on marketing: Using customer equity to focus marketing strategy. *Journal of marketing*, *68*(1), 109-127.

Sahni, Navdeep S., Christian Wheeler, and Pradeep Chintagunta (2018), "Personalization in Email Marketing: The Role of Noninformative Advertising Content", *Marketing Science*, 37(2), 236-258.

Schmitt, Julia, Klaus M. Miller, Bernd Skiera (2021), “The Impact of Privacy Laws on Online User Behavior”, Papers 2101.11366, arXiv.org.

Son, I., Lee, D., Lee, J. N., & Chang, Y. B. (2014). Market perception on cloud computing initiatives in organizations: An extended resource-based view. *Information & Management*, *51*(6), 653-669.

Sorescu, A., & Sorescu, S. M. (2016). Customer satisfaction and long-term stock returns. *Journal of Marketing*, *80*(5), 110-115.

Srinivasan, S., Pauwels, K., Silva-Risso, J., & Hanssens, D. M. (2009). Product innovations, advertising, and stock returns. *Journal of Marketing*, *73*(1), 24-43.

Steelman, Z. R., Havakhor, T., Sabherwal, R., & Sabherwal, S. (2019). Performance consequences of information technology investments: Implications of emphasizing new or current information technologies. *Information systems research*, *30*(1), 204-218.

Sutanto, Juliana, Elia Palme, Chuan-Hoo Tan, and Chee Wei Phang (2013), "Addressing the Personalization–Privacy Paradox: An Empirical Assessment from a Field Experiment on Smartphone Users", *MIS Quarterly*, 37(4), 1141-1164.

Taylor, A., & Helfat, C. E. (2009). Organizational linkages for surviving technological change: Complementary assets, middle management, and ambidexterity. *Organization Science*, *20*(4), 718-739.

The CMO Survey (2021). The Transformation of Marketing: Emerging Digital, Social, and Political Trends. *Survey Report (accessed October 17, 2021)*, Retrieved from https://cmosurvey.org/wp-content/uploads/2021/02/The_CMO_Survey-Highlights_and_Insights_Report-February-2021.pdf.

Tirunillai, S., & Tellis, G. J. (2014). Mining marketing meaning from online chatter: Strategic brand analysis of big data using latent dirichlet allocation. *Journal of marketing research*, *51*(4), 463-479.

Tsai, Janice Y., Serge Egelman, Lorrie Cranor, and Alessandro Acquisti (2011), "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study", *Information Systems Research*, 22(2), 254-268.

Tucker, Catherine E., Social Networks, Personalized Advertising, and Privacy Controls (May 6, 2014). NET Institute Working Paper No. 10-07, MIT Sloan Research Paper No. 4851-10, Available at SSRN: https://ssrn.com/abstract=1694319 or http://dx.doi.org/10.2139/ssrn.1694319

Turjeman, Dana, and Fred M. Feinberg (2019), "When the Data Are Out: Measuring Behavioral Changes Following a Data Breach", Available at SSRN: https://ssrn.com/abstract=3427254 or http://dx.doi.org/10.2139/ssrn.3427254.

Varian, H., 2019. *16. Artificial Intelligence, Economics, and Industrial Organization* (pp. 399-422). University of Chicago Press.

Venkatesan, Rajkumar, and Paul W. Farris (2012), "Measuring and Managing Returns from Retailer-Customized Coupon Campaigns", *Journal of Marketing*, 76(1), 76-94.

Venkatesan, Raj, and Jim Lecinski (2021), "*The AI Marketing Canvas: A Five-stage Road Map to Implementing Artificial Intelligence in Marketing*," Stanford University Press.

Wu, L., Hitt, L., & Lou, B. (2020). Data analytics, innovation, and firm productivity. *Management Science*, *66*(5), 2017-2039.

Xu, Heng, Hock-Hai Teo, Bernard C. Y. Tan, Ritu Agarwal (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.