



Management Science

Publication details, including instructions for authors and subscription information:
<http://pubsonline.informs.org>

The Bright Side of the GDPR: Welfare-Improving Privacy Management

Chongwoo Choe, Noriaki Matsushima, Shiva Shekhar

To cite this article:

Chongwoo Choe, Noriaki Matsushima, Shiva Shekhar (2025) The Bright Side of the GDPR: Welfare-Improving Privacy Management. *Management Science* 71(8):6836–6858. <https://doi.org/10.1287/mnsc.2024.06653>

This work is licensed under a Creative Commons Attribution 4.0 International License. You are free to copy, distribute, transmit and adapt this work, but you must attribute this work as “*Management Science*. Copyright © 2024 The Author(s). <https://doi.org/10.1287/mnsc.2024.06653>, used under a Creative Commons Attribution License: <https://creativecommons.org/licenses/by/4.0/>.”

Copyright © 2024 The Author(s)

Please scroll down for article—it is on subsequent pages



With 12,500 members from nearly 90 countries, INFORMS is the largest international association of operations research (O.R.) and analytics professionals and students. INFORMS provides unique networking and learning opportunities for individual professionals, and organizations of all types and sizes, to better understand and use O.R. and analytics tools and methods to transform strategic visions and achieve better outcomes. For more information on INFORMS, its publications, membership, or meetings visit <http://www.informs.org>

The Bright Side of the GDPR: Welfare-Improving Privacy Management

Chongwoo Choe,^a Noriaki Matsushima,^b Shiva Shekhar^{c,*}
^aDepartment of Economics, Monash University, Clayton, Victoria 3800, Australia; ^bInstitute of Social and Economic Research, Osaka University, Osaka 567-0047, Japan; ^cTilburg School of Economics and Management, Tilburg University, 5037 AB Tilburg, Netherlands

*Corresponding author

Contact: chongwoo.choe@monash.edu,  <https://orcid.org/0000-0001-6145-6907> (CC); nmatsush@iser.osaka-u.ac.jp,  <https://orcid.org/0000-0002-7865-3875> (NM); s.shekhar_1@tilburguniversity.edu,  <https://orcid.org/0000-0002-6225-5821> (SS)

Received: June 26, 2024

Accepted: October 15, 2024

Published Online in Articles in Advance:
November 21, 2024

<https://doi.org/10.1287/mnsc.2024.06653>

Copyright: © 2024 The Author(s)

Abstract. We study the General Data Protection Regulation (GDPR)’s opt-in requirement in a model with a firm that provides a digital service and consumers who are heterogeneous in their valuations of the firm’s service and the privacy costs incurred when sharing personal data with the firm. We show that the GDPR boosts demand for the service by allowing consumers with high privacy costs to buy the service without sharing data. The increased demand leads to a higher price but a smaller quantity of shared data. If the firm’s revenue is largely usage based rather than data based, then both the firm’s profit and consumer surplus increase after the GDPR, implying that the GDPR can be welfare improving. But if the firm’s revenue is largely from data monetization, then the GDPR can reduce the firm’s profit and consumer surplus.

History: Accepted by D. J. Wu, information systems.



Open Access Statement: This work is licensed under a Creative Commons Attribution 4.0 International License. You are free to copy, distribute, transmit and adapt this work, but you must attribute this work as “*Management Science*. Copyright © 2024 The Author(s). <https://doi.org/10.1287/mnsc.2024.06653>, used under a Creative Commons Attribution License: <https://creativecommons.org/licenses/by/4.0/>.”

Funding: The authors gratefully acknowledge financial support from the Australian Research Council [Grant DP210102015], the Japan Society for the Promotion of Science [KAKENHI Grants JP20H05631, JP21H00702, JP21K01452, JP21K18430, JP23H00818, JP23K20593, and JP23K25515], the Nomura Foundation, the International Joint Research Promotion Program at Osaka University, and the program of the Joint Usage/Research Center for “Behavioral Economics” at the ISER, Osaka University. Although N. Matsushima serves as a member of the Competition Policy Research Center at the Japan Fair Trade Commission (JFTC), the views expressed in this paper are solely ours and should not be attributed to the JFTC.

Supplemental Material: The online appendix is available at <https://doi.org/10.1287/mnsc.2024.06653>.

Keywords: GDPR • opt-in • opt-out • privacy management • welfare

1. Introduction

The European Union (EU)’s General Data Protection Regulation (GDPR) is generally considered to be the most stringent law that governs personal data protection and is setting a global standard for privacy regulations.¹ Before the GDPR went into effect in 2018, many consumers had little control over their data in the digital space. For example, privacy regulations such as the EU’s Data Protection Directive (Directive 95/46/EC) or Australia’s Privacy Act 1988 were based on principles and guidelines, which were nonbinding and not specific enough, nor were they entirely fit for the digital age. As a result, online businesses collected and processed personal data without providing clear information to consumers as to what data are collected, how it is used, and with whom it is shared. Data collection was often set as the default option, from which consumers could

not easily opt out. The GDPR superseded the EU’s Data Protection Directive with more specific data protection requirements, stiffer enforcements, and penalties for non-compliance. In addition, to rectify the opaque data collection process, the GDPR (Article 7, Recital 32) requires businesses to allow consumers to make a “freely given, specific, informed and unambiguous” consent to the processing of their personal data, with significant penalties for noncompliance.² This requirement essentially mandates opt-in consent to data collection. Evidence shows that opt-in results in much lower levels of participation than opt-out (Johnson et al. 2002, 2020), which may explain why opt-out was a predominant way businesses obtained consent before the GDPR.

Although the European Commission has been positive about the overall success of the GDPR,³ the media’s assessment has been mixed. Positive assessment was

based on more user control over personal data, transparency, and accountability requirements on data processors, while negative assessment pointed out the complexity and compliance costs, especially for smaller businesses, adverse effects on investment in technology ventures, as well as the GDPR's insufficient data protection measures.⁴

The academic literature has been generally more critical. A number of empirical studies report adverse effects of the GDPR on businesses such as a decrease in the amount of data collected (Schmitt et al. 2021, Congiu et al. 2022, Aridor et al. 2023) that adversely affect artificial intelligence (AI) startups and data-based innovation (Bessen et al. 2020, Batikas et al. 2023), dampened incentives to invest in technology ventures (Jia et al. 2021), decreased the number of mobile apps (Janßen et al. 2022), reduced website pageviews and e-commerce revenue (Goldberg et al. 2024), and increased market concentration in websites and web technology services (Schmitt et al. 2021, Peukert et al. 2022, Johnson et al. 2023).⁵ In addition, several theoretical studies show that the GDPR's opt-in requirement in its current form can be ineffective in allowing consumers to effectively manage their privacy (Choi et al. 2019, Chen 2022, Chaudhury and Choe 2023).

Given the negative assessment summarized above, one may wonder if there is any salutary effect to the GDPR. After all, if consumers are able to manage their privacy more effectively because of the GDPR, shouldn't they benefit from it? Or would the potential consumer benefits be skimmed away by the digital business with market power? How does the GDPR change total surplus? Answering these questions is the primary purpose of this paper.

We examine the GDPR's opt-in requirement for data collection in an environment that we believe incorporates consumer heterogeneity in a richer and more realistic way than in the existing literature on digital privacy.⁶ Specifically, we assume that consumers differ in two dimensions: in their preference for the online service under consideration and in the privacy costs incurred while sharing personal data with the online business. Adding consumer heterogeneity in privacy costs to otherwise a standard model of privacy regulation is motivated by two factors. First, growing evidence reports that consumers are highly heterogeneous in their privacy preferences (Goldfarb and Tucker 2012, Ghose 2017, Lin 2022, Macha et al. 2024). For example, Acquisti et al. (2015) review studies that classify individuals into three privacy groups: privacy fundamentalists, pragmatists, and unconcerned. Second, given that one of the stated purposes of the GDPR is to enable consumers to better manage their privacy, a model where all consumers have identical privacy preference is unlikely to yield meaningful insight. Incorporating such multidimensional consumer heterogeneity allows us to

study consumer choice in a way that is richer than in the existing literature, which allows us to identify conditions under which the GDPR can increase or decrease welfare.

We briefly sketch our model. A firm sells an online service to consumers who are heterogeneous along two dimensions, valuation for the service and privacy cost, the latter incurred if a consumer shares her personal data with the firm when using the service. If a consumer shares her data with the firm, which we call opt-in as opposed to opt-out, she can enjoy additional opt-in benefits offered by the firm. The firm can monetize the data, so that it earns revenue from two sources: sales of its service that depends on the total demand the firm faces and shared consumer data that depends only on the opt-in demand. We call the former usage-based revenue and the latter data-based revenue. The firm chooses price for its service to maximize profit, and consumers make decisions to buy the firm's service and whether to share data with the firm. We compare the equilibria before and after the GDPR.

Our basic assumption is that the GDPR enables consumers to proactively manage their digital privacy by requiring the firm to allow consumers to buy its service without sharing their personal data, that is, opt-out purchase. That is, before the GDPR, consumers must share data with the firm when buying its service but, after the GDPR, consumers can choose between opt-in and opt-out purchase. This is clearly a simplifying assumption. Even before the GDPR, some privacy-conscious consumers may bypass the firm's data collection, for example, by deleting cookies, using VPNs or privacy-oriented browsers, etc. Likewise, even after the GDPR, some consumers may routinely opt in without thinking through the ramifications of their decisions. However, insofar as more consumers rationally make opt-in decisions after the GDPR, which we believe is plausible, our main insight should continue to hold.⁷ In short, a key change brought about by the GDPR in our model is privacy management made available to consumers, who make opt-in decisions by comparing benefits from sharing data with possible privacy costs.⁸

First, we show that the equilibrium price for the firm's service increases after the GDPR. The intuition is as follows. Before the GDPR, some consumers with high privacy costs may not buy the service because they do not have an option to buy the service without sharing personal data. After the GDPR, they can participate by choosing opt-out purchase, which expands demand for the service. This allows the firm to raise prices. The additional choice of opt-out purchase and the higher price will inevitably decrease the opt-in demand, hence the amount of data shared, which will erode the firm's data-based revenue. But the effect of higher price on data-based revenue is smaller after the GDPR because the firm earns data-based revenue only

from opt-in demand after the GDPR in contrast to total demand before the GDPR. That is, the firm's choice of price is less constrained by data-based revenue after the GDPR. This implies that the firm charges a higher price for its service after the GDPR regardless of the size of its data-based revenue.

Our next result shows how the GDPR changes the equilibrium demand for the firm's service. As discussed above, the GDPR expands demand by providing consumers with an additional choice of opt-out purchase, which we call the demand expansion effect. But it leads to a higher price for the service, which counteracts the demand expansion effect. If the demand expansion effect dominates the price effect, then the equilibrium demand increases after the GDPR; otherwise, it decreases. We show that the effect of the GDPR on the equilibrium demand hinges on the firm's revenue model. When the firm's revenue is mainly from selling service and its data-based revenue is not large, the firm chooses a high price for its service close to the monopoly level. As a result, the market is not sufficiently covered before the GDPR, which leaves significant room for demand expansion after the GDPR. In this case, the demand expansion effect dominates the price effect; hence, the equilibrium demand increases after the GDPR. However, if the firm earns large data-based revenue, it chooses a low price for its service, resulting in the market sufficiently covered before the GDPR. In this case, the price effect dominates the demand expansion effect, implying that the demand increase following the GDPR is limited. Moreover, if the price increase after the GDPR is sufficiently large, then consumers with high privacy costs who purchased the service before the GDPR drop out of the market after the GDPR. As a result, the equilibrium demand can decrease after the GDPR. Although the effect of the GDPR on the total equilibrium demand depends on the firm's data-based revenue, the amount of data collected by the firm unambiguously decreases after the GDPR, consistent with empirical evidence cited earlier.

Next, we show how the firm's profit changes after the GDPR. As previously alluded to, the effect of the GDPR on profit also depends on the firm's revenue model. When the firm's revenue is largely usage based, the higher price and larger demand imply that the firm earns larger revenue after the GDPR. Although its data-based revenue decreases because the quantity of shared data decreases, the firm earns larger profit because the data-based revenue is a small part of its profit. On the other hand, the GDPR can erode the firm's profitability if its revenue is largely data based because, in this case, the GDPR leads to limited demand expansion but has a large negative effect on the quantity of data collected. The implication is that the GDPR's effect on the firm's profit depends on the firm's business model. The GDPR is likely to benefit

usage-driven businesses such as ride-hailing platforms like Uber or streaming services like Netflix but hurt data-driven businesses such as various navigation and weather apps and, to some extent, businesses whose main revenue source is advertising that leverages user data.

The GDPR's effect on consumer surplus also hinges on whether the firm's revenue is largely usage based or data based. In the former case, the GDPR's demand expansion effect dominates the price effect. Given that more consumers can participate in the market after the GDPR while benefiting from more effective privacy management, consumer surplus increases in this case. However, when the firm earns significant data-based revenue, the price effect dominates the demand expansion effect, and the equilibrium demand can decrease. Thus, consumer surplus decreases in this case. Once again, the implication is that the GDPR can benefit consumers in markets that are largely service based but can hurt consumers when data-based revenue is a significant part of digital business. Given that total surplus is the sum of profit and consumer surplus, the GDPR's effect on total surplus parallels its effect on profit and consumer surplus. Namely, the GDPR is likely to improve welfare in usage-driven businesses but reduce welfare in data-driven businesses.

Although the GDPR's opt-in requirement is the main focus of this paper, the way we describe privacy management made available after the GDPR applies more generally to other online businesses as well. In many e-retailers such as Target, Walmart, Zara, and so on, consumers can choose to create an account for transaction or check out as a guest without creating an account. By creating an account, consumers share various personal data with the retailer. The benefits of creating an account include faster checkout, order tracking, and exclusive deals and promotions. On the other hand, sharing data with e-retailers can pose privacy risks such as identity theft, data breaches, cyberstalking, and so on. The option to manage privacy is available on other platforms such as Google and YouTube. Users can choose the incognito mode or delete usage history after using services provided by these platforms. Once again, privacy management trades off additional benefits from sharing data against possible privacy risks. The general conclusion from our analysis is that, for digital businesses that do not rely heavily on data-based revenue, empowering consumers to proactively manage their digital privacy can improve firm profitability, increase consumer surplus, and hence is welfare-improving. But effective privacy management by consumers can reduce welfare when businesses rely heavily on data-based revenue.⁹ We stress that this conclusion applies where consumers can effectively manage their privacy. But this may not necessarily be the case even after the GDPR, as we discuss in Section 6.5.

The rest of the paper is organized as follows. In Section 2, we review the related literature. Section 3 presents our baseline model. Section 4 analyzes the baseline model, and Section 5 provides our key welfare results. In Section 6, we discuss several extensions and variations of the baseline model and provide the discussions on testable hypotheses and management implications. Section 7 concludes the paper. The appendix contains the analysis of a general model that encompasses the baseline model studied in Sections 4 and 5. All missing proofs are relegated to the Online Appendix.

2. Related Literature

Our work is related to a number of theoretical studies that model some of the key features of the GDPR and examine the digital business's optimal strategy and welfare implications. Choi et al. (2019) focus on the GDPR's opt-in requirement when there are data externalities and show that the monopolistic firm can render opt-in regulations ineffective if it can exercise price discrimination. In deriving this result, they assume full market coverage, whereas we consider the case where the firm uses uniform pricing and the market is not fully covered. Fainmesser et al. (2023) study the digital business's choice of data collection and data security and show how the optimal strategy depends on the digital business's revenue model, that is, whether it is more usage driven or data driven. But the digital business's optimal pricing decision is absent in their model, and consumers do not explicitly make opt-in decisions. Ke and Sudhir (2023) analyze a model of behavior-based pricing that endogenizes the consumer's decision to exercise the rights to opt-in, data erasure, and data portability, and firms can offer personalized products to opt-in consumers. In their model, data erasure and portability imply that only opt-in decisions arise in equilibrium.¹⁰ Chen (2022) studies socially optimal data collection policy when consumers differ in privacy costs. Chaudhury and Choe (2023) provide an illustrative example of optimal data policy when consumers differ in privacy costs and there are multiple data types. Although not directly related to the GDPR, Campbell et al. (2015) show that a consent requirement in privacy regulation can tilt the playing field in favor of large generalist firms at the cost of small, specialist firms, because it imposes a one-off cost on both, but consumer data have multiple uses in the former. In addition to the differences already explained above, none of these studies model multidimensional consumer heterogeneity as we do in this paper.

A large and growing body of literature studies consumers' privacy choice and the attendant data externalities (Choi et al. 2019; Ichihashi 2021, 2023; Acemoglu et al. 2022; Bergemann et al. 2022).¹¹ A general conclusion from these studies is that opt-in consumers allow

the data controller to infer more information about opt-out consumers, which can lead to excessive data sharing and raise the cost from privacy breach.¹² Once again, the main difference between these studies and ours is that we explicitly model multidimensional consumer heterogeneity, whereas consumers differ only in one dimension in these studies, for example, in their valuation of the digital business's service (Choi et al. 2019, Bergemann et al. 2022) or in their valuation of privacy (Acemoglu et al. 2022, Ichihashi 2023).

Several studies model multidimensional consumer types as we do in this paper, although their focus is different from ours (Anderson and Gans 2011, Jentzsch et al. 2013, Miklós-Thal et al. 2024). Anderson and Gans (2011) model consumer heterogeneity in preference and disutility from advertising in the media market. In the oligopoly model of product differentiation in Jentzsch et al. (2013), consumers differ in brand preference and transportation costs. Miklós-Thal et al. (2024) study consumers' privacy choice when each consumer is represented by two data types: privacy-sensitive data and innocuous data. Methodologically, the way we model opt-out is close to the choice of ad avoidance in Anderson and Gans (2011). That is, consumers in our model can choose opt-out purchase to avoid privacy costs, although they lose the opt-in benefits by doing so.

3. Model

We consider a digital business that provides an online service at zero marginal cost and charges price p . Consumers are heterogeneous along two dimensions: valuation for the service (v) and privacy cost (c). We interpret c to be the maximum possible privacy cost the consumer incurs when sharing data with the firm.¹³ We assume v and c are independent and are uniformly distributed on $[0, 1]$.¹⁴ Consumers face three possible choices: buying the service while sharing data, called opt-in purchase; buying the service without sharing data, called opt-out purchase; and not buying the service.¹⁵ Denote the mass of consumers choosing opt-in purchase by D_S , the mass of consumers choosing opt-out purchase by D_N , and the total demand for the firm's service by $D = D_S + D_N$.

The firm can further enhance its service by offering additional benefits to consumers who choose opt-in purchase. We call this opt-in benefits denoted by $x \in (0, 1)$.¹⁶ The opt-in benefits include, among others, time saved thanks to faster checkout, exclusive deals and promotions, improved and personalized service, and so on. To focus squarely on the GDPR's effect on the demand for the firm's service, we assume x is exogenously given and is provided at no additional cost.¹⁷ Thus, the main strategic variable the firm chooses in our model is price for its service.

We choose price as the firm's strategic variable in order to present a model that can encompass usage-based and

data-based digital businesses in a unified framework, which facilitates the comparison of how the GDPR impacts these businesses. In reality, some data-driven businesses, for example, in search and social media, provide “free” services in return for user data they monetize, and they rely on additional strategic variables such as the investment in technology and innovation and various data monetization strategies. But the fact that they provide “free” service, hence a zero price, does not mean price does not play a role.¹⁸ A zero price can be an optimal choice for businesses with significant data-based revenue. As the GDPR makes data collection more difficult, many data-driven businesses depart from the zero price policy, which further indicates the importance of price as a strategic variable for these businesses.¹⁹

A consumer of type $(v, c) \in [0, 1]^2$ who chooses opt-in purchase receives utility

$$U_S(v, c) := v + \underbrace{(x - c)}_{\text{net opt-in benefits}} - p, \quad (1)$$

where p is the price charged by the firm, and $x - c$ is the opt-in benefits less privacy cost. If a type (v, c) consumer chooses an opt-out purchase, then her utility is

$$U_N(v, c) := v - p. \quad (2)$$

Clearly, the main difference between opt-in and opt-out purchase is that a consumer choosing opt-in purchase expects the additional opt-in benefits as well as privacy costs. As discussed in Section 1, a key change brought about by the GDPR is that firms need explicit opt-in consent from consumers in order to collect data. Our interpretation of this in our model is that consumers can choose between opt-in and opt-out purchase after the GDPR, although they cannot choose opt-out purchase before the GDPR. Based on this, we can summarize a consumer’s decision as follows. Before the GDPR, a consumer buys the firm’s service if $U_S \geq 0$. After the GDPR, she chooses opt-in purchase if $U_S \geq \max\{U_N, 0\}$, opt-out purchase if $U_N \geq \max\{U_S, 0\}$, and no purchase otherwise.

The firm’s revenue comes from two sources. First, the firm earns revenue from sales of its service. Given the total demand for the firm’s service $D(\cdot)$, its sales revenue is $pD(\cdot)$. Second, the firm can monetize the data it collects, for example, through selling data for targeted advertising (Bergemann and Bonatti 2015), using data for personalized pricing (Choe et al. 2018, Chen et al. 2020), or through product improvement by data-enabled learning (Hagiu and Wright 2023). We do not model how the firm monetizes its data and simply assume that the revenue is exogenously given by $\alpha \geq 0$ per unit of consumer data. Given that the firm collects data from all opt-in consumers whose mass is denoted by $D_S(\cdot)$, the firm’s revenue from data are $\alpha D_S(\cdot)$.

Noting that we assume away all costs for the firm, the firm’s profit is given by

$$\Pi = \underbrace{pD(\cdot)}_{\text{sales revenue}} + \underbrace{\alpha D_S(\cdot)}_{\text{data-based revenue}}. \quad (3)$$

Before the GDPR, we have $D_N = 0$; hence, $D = D_S$. Therefore, the main difference in the firm’s profit after the GDPR is the possibility that $D > D_S$.

The game proceeds as follows. First, consumers learn their types privately. Next, the firm chooses p to maximize profit given in (3), which is followed by consumers’ decisions: Before the GDPR, consumers make only purchase decisions; after the GDPR, they make additional data-sharing decisions.

In the remainder of this section, we offer discussions on our assumption that opt-out purchase is not available before the GDPR. In case the firm is better off by offering both opt-in and opt-out purchase options to consumers, one may ask why it does not do so before the GDPR. We argue that the lack of stringent enforcement before the GDPR implies that the firm could not credibly commit not to gather data from consumers who choose opt-out purchase. As explained earlier, privacy regulations in Europe before the GDPR were largely based on general guidelines and principles, and enforcement mechanisms and penalties for noncompliance were left to the discretion of individual EU member states. Regarding the consent requirement for data collection, some member states such as France and Germany required consent for data processing, while others were not explicit about consent requirements. But even when the fine was imposed for breach, it was substantially smaller than what was imposed after the GDPR. For example, the French privacy watchdog (CNIL) imposed 150,000 euros on Google in 2014 for failing to provide clear and comprehensive information to users and for not obtaining their consent before storing cookies on their devices.²⁰ This is in stark contrast to the significant penalties introduced after the GDPR.²¹

Our argument can be formalized by considering a simple sequential-move game as follows. In the first stage, the firm offers an opt-out purchase option in addition to an opt-in purchase option. In the second stage, consumers make purchase decisions and decide which option to choose. In the final stage, the firm decides whether to monetize data from consumers who chose opt-out purchase. If monetizing data from opt-out consumers incurs an expected penalty smaller than the revenue from data monetization, then the firm chooses to monetize data. Then, by backward induction, consumers do not choose opt-out purchase in the second stage simply because the firm’s offer of opt-out purchase option is not credible. Consequently, they face only two effective choices: opt-in purchase or no purchase. This is our interpretation of the privacy

regime before the GDPR. The main thrust of the GDPR is that it lends credibility to the firm's offer of opt-out purchase option thanks to its stricter enforcement and significant penalties for infringement.

4. Analysis

4.1. Equilibrium Before the GDPR

Because consumers cannot choose opt-out purchase in this case, any consumer who buys the firm's service also shares her data with the firm. Thus, consumer utility relevant to her purchase decision is $U_S(v, c)$.

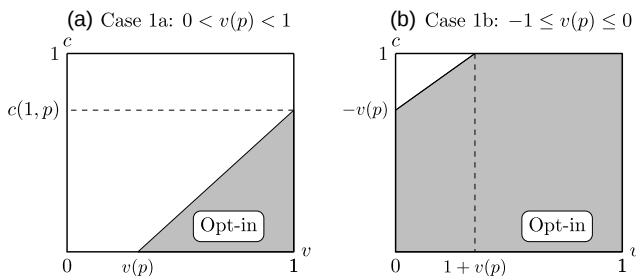
A consumer of type (v, c) buys the service if and only if

$$U_S(v, c) \geq 0 \Rightarrow c \leq c(v, p) := v + x - p.$$

In the above, $c(v, p)$ is the privacy cost that makes the consumer indifferent between opt-in purchase and no purchase given her valuation v and price p . Then, $c(1, p) = 1 + x - p$ is the threshold value of privacy cost above which there is no demand for the service. Likewise, $v(p) := p - x$ is the threshold value of consumer valuation for the service, below which there is no demand for the service.

Depending on $v(p) > 0$ or $v(p) \leq 0$, there are two possible cases, as shown in Figure 1. First, the demand for the case where $0 < v(p) < 1$, that is, $x < p < 1 + x$, is illustrated in Figure 1(a), which we call case 1a. This is the case where some consumers with low valuation for the service do not purchase the service regardless of their privacy costs. This case arises when the price is higher than the opt-in benefits. Second, Figure 1(b) shows the demand for the case where $-1 \leq v(p) \leq 0$, or $x - 1 \leq p \leq x$, which we call case 1b.²² This is the case where the opt-in benefits are large enough ($x \geq p$) so that all consumers with relatively low privacy costs purchase the service, regardless of their valuation for the service. But the opt-in benefits are not too large ($x < 1 + p$) so that some consumers with high privacy costs and low valuation do not purchase the service. In case 1b, a subset of consumers along one dimension of consumer types is fully served but not along the other dimension. Thus, a case like this is possible only when consumer types are multidimensional.

Figure 1. Demand Before the GDPR



From the above, we can calculate the demand for the firm's service as²³

$$\begin{aligned} \hat{D}(\hat{p}) &= \begin{cases} \int_{v(\hat{p})}^1 \int_0^{c(v, \hat{p})} dc dv = \frac{(1+x-\hat{p})^2}{2} & \text{if } x < \hat{p} < 1+x, \\ \int_0^{1+v(\hat{p})} \int_0^{c(v, \hat{p})} dc dv + \int_{1+v(\hat{p})}^1 \int_0^1 dc dv = 1 - \frac{(1-x+\hat{p})^2}{2} & \text{if } x-1 \leq \hat{p} \leq x. \end{cases} \end{aligned} \quad (4)$$

The firm chooses $\hat{p}$ to maximize $\hat{\Pi}(\hat{p}) = (\hat{p} + \alpha)\hat{D}(\hat{p})$, leading to the following first-order condition:

$$\frac{\partial \hat{\Pi}(\hat{p})}{\partial \hat{p}} = \underbrace{\hat{D}(\hat{p})}_{\text{Margin effect (+)}} + \underbrace{p \frac{\partial \hat{D}(\hat{p})}{\partial \hat{p}}}_{\text{Volume effect (-)}} + \underbrace{\alpha \frac{\partial \hat{D}(\hat{p})}{\partial \hat{p}}}_{\text{Data Volume effect (-)}} = 0.$$

Apart from the tradeoff between classical margin and volume effects the firm faces in choosing price, the presence of data-based revenue reduces the firm's incentive to increase price. If $\alpha = 0$, then we have the standard monopoly problem. Given $\partial \hat{D} / \partial \hat{p} < 0$, the firm will set price lower than the monopoly price when it earns data-based revenue.

We can solve the first-order condition for the equilibrium price $\hat{p}^*$.²⁴ In equilibrium, the conditions for case 1a and case 1b can be restated in terms of α . Specifically, case 1a arises for small values of α and case 1b for large values of α . In the appendix, we show that case 1a corresponds to the range of α such that $\alpha < \alpha_1(x) := \max\{(1-2x)/2, 0\}$, and case 1b corresponds to the range of α such that $\alpha \geq \alpha_1(x)$. Intuitively, when α is small, the firm chooses a high price close to the monopoly level, which leaves a large part of the market uncovered. As α increases, the firm's optimal price decreases, which in turn increases the equilibrium demand.

The analytical results can be complicated due to multidimensional consumer types. In order to provide the key insight as clearly as we can, we report the results for the case $x = 1/4$ in the main text. As will become clear below, the case $x = 1/4$ admits all possible equilibria in our model, which allows us to explain our main results at little loss of generality.²⁵ This allows us to express the equilibrium in terms of α only and discuss how the impact of the GDPR differs depending on the firm's revenue model, that is, different values of α . We then calculate how the equilibrium changes as the value of α changes, based on which to explain our main results. In the appendix, we provide the detailed analytical steps for all the results in the main text for general values of x and α , showing that our results can be generalized. Therefore, we omit the proof of the results in Section 4.

When $x = 1/4$, the threshold value of α that divides case 1a and case 1b is given by $\alpha = 1/4$, which is shown in the appendix. Solving the firm's problem for $\hat{p}^*$, and deriving the equilibrium demand $\hat{D}^*$, profit $\hat{\Pi}^*$, and consumer surplus $\widehat{CS}^*$, we obtain the following.

Lemma 1. When $x = 1/4$, the equilibrium before the GDPR can be characterized as follows.

• If $\alpha < 1/4$, then we have case 1a where the equilibrium price, demand, profit, and consumer surplus are given as

$$\hat{p}^* = \frac{1}{12}(5 - 8\alpha), \hat{D}^* = \frac{2}{9}\left(\frac{5}{4} + \alpha\right)^2, \hat{\Pi}^* = \frac{2}{27}\left(\frac{5}{4} + \alpha\right)^3, \\ \widehat{CS}^* = \frac{4}{81}\left(\frac{5}{4} + \alpha\right)^3.$$

• If $\alpha \geq 1/4$, then we have case 1b where the equilibrium price, demand, profit, and consumer surplus are given as

$$\hat{p}^* = \frac{1}{3}\left(-\frac{3}{2} - \alpha + \beta\right), \hat{D}^* = \frac{1}{9}\left(6 - \left(\alpha - \frac{3}{4}\right)^2 + \left(\alpha - \frac{3}{4}\right)\beta\right), \\ \hat{\Pi}^* = \frac{1}{27}\left(2\alpha - \frac{3}{2} + \beta\right)\left(6 - \left(\alpha - \frac{3}{4}\right)^2 + \left(\alpha - \frac{3}{4}\right)\beta\right), \\ \widehat{CS}^* = \frac{1}{81}\left(81 + 18\left(\alpha - \frac{3}{4}\right) - 2\left(\alpha - \frac{3}{4}\right)^3 \right. \\ \left. - 2\left(12 - \left(\alpha - \frac{3}{4}\right)^2\right)\beta\right),$$

where $\beta = \sqrt{6 + (\alpha - 3/4)^2}$.

It is easy to check from the above lemma that the equilibrium price decreases in α but the equilibrium demand, profit, and consumer surplus all increase in α . This is intuitively clear. When α increases, the firm can benefit more by increasing the volume of data, from which it earns data-based revenue. Thus, it reduces price to attract more consumers. A lower price and larger demand imply that consumer surplus increases in α . In addition, because the firm's equilibrium profit changes in response to a change in α exactly by the amount of its equilibrium demand, a direct consequence of the envelope theorem,

the firm's profit also increases in α . Finally, we note that the equilibrium price can be negative when α is large enough. Nonetheless, the equilibrium profit increases in α because of larger data-based revenue.

Table 1 shows how the equilibrium price, demand, profit, and consumer surplus change when α increases. For $\alpha \leq 0.25$, we have case 1a equilibrium outcomes and, for $\alpha > 0.25$, we have case 1b equilibrium outcomes, which is indicated in the second column. As shown in the table, the equilibrium price decreases in α but the equilibrium demand, profit, and consumer surplus all increase in α . The equilibrium price is equal to zero when $\alpha = 0.958$ and becomes negative thereafter. This confirms our earlier explanation that, when the firm earns large data-based revenue, it can be optimal to pay consumers to use its service and monetize data thus collected.²⁶

4.2. Equilibrium After the GDPR

After the GDPR, a consumer of type (v, c) chooses opt-in purchase if $U_S \geq \max\{U_N, 0\}$, opt-out purchase if $U_N \geq \max\{U_S, 0\}$, and no purchase if $\max\{U_S, U_N\} \leq 0$. Thus, the set of consumers choosing opt-in purchase is given by

$$\{(v, c) \in [0, 1]^2 \mid c \leq v + x - p, x \geq c\},$$

and the set of consumers choosing opt-out purchase is given by

$$\{(v, c) \in [0, 1]^2 \mid v \geq p, x < c\}.$$

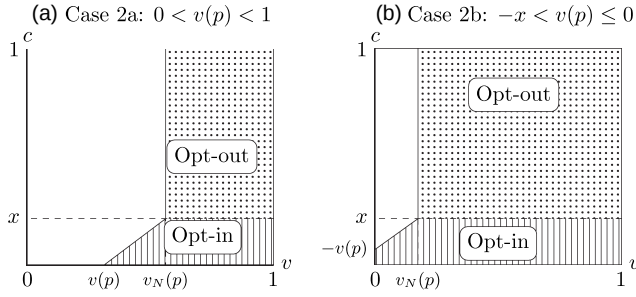
As before, $U_S \geq 0$ leads to the threshold condition: $c \leq c(v, p) = v + x - p$. Then, $v(p) = p - x$ is the threshold value of consumer valuation for the service, below which no consumers choose opt-in purchase. Next, $U_N \geq 0$ if $v \geq p$, which leads to $v_N(p) := p$, the threshold value of consumer valuation, below which no consumers choose opt-out purchase. Clearly, we have $v(p) \leq v_N(p)$. In addition, $U_S \geq U_N$ holds if and only if $x \geq c$.

Once again, we have two possible cases, depending on $v(p) > 0$ or $v(p) \leq 0$. These are depicted in Figure 2, where the area labeled opt-in represents the demand from consumers who choose opt-in purchase, and the

Table 1. Equilibrium Outcome Before the GDPR

α	Case	Price	Demand	Profit	Consumer surplus	Total surplus
0	1a	0.417	0.347	0.145	0.096	0.241
0.1	1a	0.350	0.405	0.182	0.122	0.304
0.2	1a	0.283	0.467	0.226	0.151	0.376
0.25	1b	0.250	0.500	0.250	0.167	0.417
0.4	1b	0.191	0.557	0.329	0.198	0.527
0.5	1b	0.154	0.591	0.387	0.219	0.606
0.958	1b	0	0.719	0.689	0.320	1.009
2.5	1b	-0.330	0.912	1.979	0.592	2.571
3.5	1b	-0.439	0.952	2.913	0.694	3.607
4.5	1b	-0.507	0.970	3.875	0.759	4.634

Figure 2. Demand After the GDPR



area labeled opt-out is the demand from consumers who choose opt-out purchase. Panel (a) illustrates the demand for case 2a where $0 < v(p) < 1$, which boils down to $x < p \leq 1$.²⁷ Panel (b) shows the demand for case 2b where $-x < v(p) \leq 0$, that is, $0 \leq p \leq x$.²⁸ As expected, the additional opt-out purchase made available by the GDPR allows consumers to self-select themselves: Those with low privacy costs choose opt-in purchase in order to enjoy the opt-in benefits; those with high privacy costs choose opt-out purchase to avoid the privacy costs.

From the above, we can calculate the opt-in, opt-out, and total demands as follows. First, the opt-in demand is

$$\begin{aligned} \tilde{D}_S(\tilde{p}) &= \begin{cases} \int_{v(\tilde{p})}^{v_N(\tilde{p})} \int_0^{c(v, \tilde{p})} dc dv + \int_{v_N(\tilde{p})}^1 \int_0^x dc dv = \frac{x^2}{2} + x(1 - \tilde{p}) & \text{if } x < \tilde{p} \leq 1, \\ \int_0^{v_N(\tilde{p})} \int_0^{c(v, \tilde{p})} dc dv + \int_{v_N(\tilde{p})}^1 \int_0^x dc dv = x - \frac{\tilde{p}^2}{2} & \text{if } 0 \leq \tilde{p} \leq x. \end{cases} \end{aligned} \quad (5)$$

The opt-out demand is zero when $1 < \tilde{p} < 1 + x$. In the other two cases, the expression for the opt-out demand is the same in both cases and is given by

$$\tilde{D}_N(\tilde{p}) := \int_{v_N(\tilde{p})}^1 \int_x^1 dc dv = (1 - x)(1 - \tilde{p}). \quad (6)$$

The total demand is then

$$\begin{aligned} \tilde{D}(\tilde{p}) &= \tilde{D}_S(\tilde{p}) + \tilde{D}_N(\tilde{p}) \\ &= \begin{cases} \frac{x^2}{2} + 1 - \tilde{p} & \text{if } x < \tilde{p} \leq 1, \\ 1 - (1 - x)\tilde{p} - \frac{\tilde{p}^2}{2} & \text{if } 0 \leq \tilde{p} \leq x. \end{cases} \end{aligned} \quad (7)$$

The firm chooses $\tilde{p}$ to maximize $\tilde{\Pi}(\tilde{p}) = \tilde{p}\tilde{D}(\tilde{p}) + \alpha\tilde{D}_S(\tilde{p})$. Compared with the problem before the GDPR, the firm's profit comes from two different sources. Its revenue

from sales depends on the total demand, but the data-based revenue depends only on the opt-in demand. As before, we can restate the conditions for case 2a and case 2b in terms of α in equilibrium. Consistent with the case before the GDPR, case 2a arises for small values of α and case 2b for large values of α . In the appendix, we show that case 2a corresponds to the range of α such that $\alpha < \alpha_2(x) := \max\{(2 - 4x + x^2)/(2x), 0\}$, and case 2b corresponds to the range of α such that $\alpha \geq \alpha_2(x)$. Moreover, one can verify that $\alpha_1(x) \leq \alpha_2(x)$ for all $x \in (0, 1)$, which implies that there are three possible pairs of pre- and post-GDPR equilibria for any α : (case 1a, case 2a) if $\alpha < \alpha_1(x)$; (case 1b, case 2a) if $\alpha \in [\alpha_1(x), \alpha_2(x)]$; (case 1b, case 2a) if $\alpha \geq \alpha_2(x)$.

In comparing the equilibria before and after the GDPR, we continue to focus on the case where $x = 1/4$. Then, the value of α that divides cases 2a and 2b is given by $\alpha = 17/8$, which is shown in the appendix. Solving the firm's problem for $\tilde{p}^*$, and deriving the equilibrium demands $\tilde{D}_S^*$, $\tilde{D}_N^*$, profit $\tilde{\Pi}^*$, and consumer surplus $\tilde{CS}^*$, we obtain the following.

Lemma 2. When $x = 1/4$, the equilibrium after the GDPR can be characterized as follows.

• If $\alpha < 17/8$, then we have case 2a where the equilibrium price, demands, profit, and consumer surplus are given as

$$\begin{aligned} \tilde{p}^* &= \frac{1}{64}(33 - 8\alpha), \quad \tilde{D}_S^* = \frac{1}{16}\left(\frac{39}{16} + \frac{\alpha}{2}\right), \quad \tilde{D}_N^* = \frac{3}{16}\left(\frac{31}{16} + \frac{\alpha}{2}\right), \\ \tilde{\Pi}^* &= \frac{1}{16}\left(\frac{1089}{256} + \frac{39\alpha}{16} + \frac{\alpha^2}{4}\right), \quad \tilde{CS}^* = \frac{1}{96}\left(\frac{3319}{256} + \frac{99\alpha}{16} + \frac{3\alpha^2}{4}\right). \end{aligned}$$

• If $\alpha \geq 17/8$, then we have case 2b where the equilibrium price, demands, profit, and consumer surplus are given as

$$\begin{aligned} \tilde{p}^* &= \frac{1}{3}\left(\Gamma - \alpha - \frac{3}{2}\right), \quad \tilde{D}_S^* = \Gamma\left(\frac{3 + 2\alpha}{18}\right) - \frac{1}{9}(\alpha^2 + 3\alpha + 3), \\ \tilde{D}_N^* &= \frac{1}{4}\left(\frac{9}{2} + \alpha - \Gamma\right), \\ \tilde{\Pi}^* &= \frac{\Gamma}{27}\left(\alpha^2 + 3\alpha + \frac{33}{4}\right) - \frac{\alpha^2}{3} - \frac{\alpha}{12} - \frac{3}{4}, \\ \tilde{CS}^* &= \frac{17}{32} + \frac{\delta}{648}(-216 + 27\delta + 4\delta^2), \end{aligned}$$

where $\Gamma = \sqrt{6 + (\alpha + 3/2)^2}$ and $\delta = \Gamma - \alpha - 3/2$.

The comparative statics of the equilibrium is similar to that for the case before the GDPR. It is easy to check from the above that the equilibrium price is decreasing in α but the equilibrium opt-in and opt-out demands, profit, and consumer surplus are all increasing in α . To facilitate the comparison with the case before the GDPR, we provide Table 2, where we show the equilibrium outcomes after the GDPR for various values of α . We have case 2a equilibrium when $\alpha < 17/8 = 2.215$ and case 2b equilibrium when $\alpha \geq 2.215$, which is

Table 2. Equilibrium Outcome After the GDPR

α	Case	Price	Opt-in demand	Opt-out demand	Profit	Consumer surplus	Total surplus
0	2a	0.516	0.152	0.363	0.266	0.135	0.401
0.1	2a	0.503	0.155	0.373	0.281	0.142	0.423
0.2	2a	0.491	0.159	0.382	0.297	0.148	0.445
0.25	2a	0.484	0.160	0.387	0.305	0.152	0.457
0.4	2a	0.466	0.165	0.401	0.329	0.162	0.491
0.5	2a	0.453	0.168	0.410	0.346	0.169	0.515
2.215	2b	0.245	0.220	0.566	0.680	0.311	0.990
2.5	2b	0.230	0.224	0.577	0.743	0.322	1.065
3.5	2b	0.189	0.232	0.608	0.971	0.356	1.327
4.5	2b	0.160	0.237	0.630	1.206	0.381	1.587

indicated in the second column. As shown in the table, the equilibrium price decreases in α but the equilibrium demands, profit, and consumer surplus all increase in α . In addition, the equilibrium price is always nonnegative after the GDPR, as explained earlier.

5. Comparing the Equilibria Before and After the GDPR

This section compares the equilibria before and after the GDPR and discusses the welfare implications of the GDPR. Our discussions are based on the results from the previous section, that is, the case where $x = 1/4$. But the qualitative results hold for general values of x , which is shown in the appendix. Thus, we omit the formal proof of the results in this section.

The preceding analysis shows that, before the GDPR, we have case 1a equilibrium if $\alpha < 1/4$ and case 1b equilibrium if $\alpha \geq 1/4$. After the GDPR, we have case 2a equilibrium if $\alpha \leq 17/8$ and case 2b equilibrium if $\alpha > 17/8$. Thus, we can identify three pairs of equilibria as follows: (i) if $\alpha < 1/4$, then we have case 1a equilibrium before the GDPR and case 2a equilibrium after the GDPR; (ii) if $1/4 \leq \alpha \leq 17/8$, then we have case 1b equilibrium before the GDPR and case 2a equilibrium after the GDPR; and (iii) if $17/8 < \alpha$, then we have case 1b equilibrium before the GDPR and case 2b equilibrium after the GDPR. This is shown in Figure 3, where the vertical dashed line corresponds to $x = 1/4$, the case where the results in Sections 4 and 5 are from.

Our first result is that the equilibrium price increases after the GDPR. It is because the GDPR enables consumers to better manage their privacy, which leads to a larger demand. To see this more closely, suppose a consumer of type (v, c) does not purchase the service before the GDPR when the price is p . This implies $v + x < p + c$. After the GDPR, the consumer can choose opt-out purchase if $v \geq p$. On the other hand, a consumer who buys the service before the GDPR will continue to do so at the same price after the GDPR; the only difference is that she will choose opt-out purchase if $v + x > p + c$ but $x < c$. Put together, we can conclude that, at any given price, the firm faces a weakly larger

demand after the GDPR. This allows the firm to raise price. A higher price can erode the firm's data-based revenue by reducing the amount of data shared. But the effect is smaller after the GDPR because the firm earns data-based revenue only from the opt-in demand after the GDPR whereas its data-based revenue is from the total demand before the GDPR. Consequently, the firm is less constrained by data-based revenue after the GDPR. Thus, it charges a higher price after the GDPR irrespective of the size of its data-based revenue.

Proposition 1. *The equilibrium price is higher after the GDPR, that is, $\Delta p^* = \hat{p}^* - \tilde{p}^* > 0$.*

In Table 3, we compare the equilibrium prices for various values of α . These prices can be found in Tables 1 and 2. As noted above, the comparison is between case 1a equilibrium and case 2a equilibrium if $\alpha < 1/4$, which is shown in the first three rows in Table 3. If $1/4 \leq \alpha < 17/8 = 2.215$, then the comparison is between case 1b equilibrium and case 2a equilibrium, which is shown in the next two rows. In the rest of Table 3, the comparison is between case 1b equilibrium and case 2b equilibrium because $\alpha \geq 17/8$. As shown in the table, the equilibrium price is always higher after the GDPR.

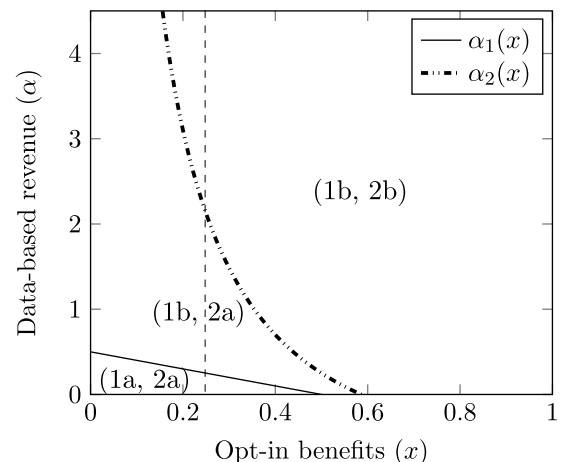
Figure 3. Different Pairs of Equilibria

Table 3. Comparison of Equilibrium Prices

α	Equilibrium pair	Price before the GDPR	Price after the GDPR
0	(case 1a, case 2a)	0.417	0.516
0.1	(case 1a, case 2a)	0.350	0.503
0.2	(case 1a, case 2a)	0.283	0.491
0.25	(case 1b, case 2a)	0.250	0.484
0.4	(case 1b, case 2a)	0.191	0.466
0.5	(case 1b, case 2a)	0.154	0.453
2.5	(case 1b, case 2b)	−0.330	0.230
3.5	(case 1b, case 2b)	−0.439	0.189
4.5	(case 1b, case 2b)	−0.507	0.160

Our next result shows how the GDPR changes the equilibrium demand. Other things equal, the GDPR should expand demand because, as explained above, it provides consumers with an additional choice of opt-out purchase. We call this the demand expansion effect. But the price increase following the GDPR as shown in Proposition 1 acts as a countervailing force, which we call the price effect. Because the pre-GDPR equilibrium price decreases in α , the price effect can be large when α is large. If the price effect more than offsets the demand expansion effect, then the GDPR can reduce the equilibrium demand; otherwise, it will increase the equilibrium demand. When α is small, say $\alpha < 1/4$, we have case 1a equilibrium before the GDPR and case 2a equilibrium after the GDPR. This is the case where the market is not sufficiently covered before the GDPR. Thus, there is significant room for demand expansion. Consequently, the demand expansion effect dominates the price effect, implying that the equilibrium demand increases after the GDPR. When α is large, however, the market is sufficiently covered before the GDPR, hence there is not much room for demand expansion. In addition, large α implies a large price effect. In this case, we expect the price effect to dominate the demand expansion effect and, accordingly, the equilibrium demand decreases after the GDPR.

Although the effect of the GDPR on the total equilibrium demand hinges on α , the effect of the GDPR on the amount of data shared is unambiguously negative. That is, the equilibrium opt-in demand after the GDPR

is always smaller than the total equilibrium demand before the GDPR. The intuition is clear. Given the additional choice of opt-out purchase made available after the GDPR, some consumers with high privacy costs who purchased the service before the GDPR can switch to opt-out purchase after the GDPR. This implies that, even when the GDPR increases the total equilibrium demand, we expect the demand from consumers who choose opt-in purchase to be smaller than that before the GDPR. As discussed previously, the negative effect of the GDPR on the amount of data collected is well documented. We also note that the marginal consumer with the lowest privacy cost who shares data has a higher valuation for the service after the GDPR, that is, $\tilde{v}^* > \hat{v}^*$. This follows directly from Proposition 1 because $\tilde{v}^* = \tilde{p}^* - x > \hat{p}^* - x = \hat{v}^*$. This is more or less consistent with the empirical findings in Aridor et al. (2023) that, although the GDPR has resulted in a reduction in total cookies, the consumers who continue to be tracked after the GDPR tend to be more valuable to advertisers.²⁹

Proposition 2. Comparing the equilibria before and after the GDPR, we find the following.

- There is a threshold value $\alpha_1 \in [1/4, 17/8]$ such that the total demand is larger after the GDPR if $\alpha \leq \alpha_1$ but smaller after the GDPR if $\alpha \geq \alpha_1$, that is, $\Delta D^* = (\tilde{D}_S^* + \tilde{D}_N^*) - \hat{D}^* \geq 0$ if and only if $\alpha \leq \alpha_1$.
- For all α , the opt-in demand after the GDPR is smaller than the total demand before the GDPR, that is, $\hat{D}^* > \tilde{D}_S^*$.
- For all α , the marginal consumer with lowest privacy cost who shares data has a higher valuation for the service after the GDPR, that is, $\tilde{v}^* > \hat{v}^*$.

In Table 4, we compare the equilibrium demands for various values of α based on Tables 1 and 2. The total demand is larger after the GDPR for all α that leads to case 1a equilibrium before the GDPR and case 2a equilibrium after the GDPR. But it is smaller for all α that leads to case 2b equilibrium after the GDPR. Although not shown in the table, the threshold value at which $\Delta D^* = 0$ is given by $\alpha_1 \approx 0.438$. We also note that, for all values of α , the opt-in demand after the GDPR is smaller than the total demand before the GDPR.

Table 4. Comparison of Equilibrium Demands

α	Equilibrium pair	Before the GDPR		After the GDPR	
		Total demand	Opt-in demand	Opt-out demand	Total demand
0	(case 1a, case 2a)	0.347	0.152	0.363	0.516
0.1	(case 1a, case 2a)	0.405	0.155	0.373	0.528
0.2	(case 1a, case 2a)	0.467	0.159	0.382	0.541
0.25	(case 1b, case 2a)	0.500	0.160	0.387	0.547
0.4	(case 1b, case 2a)	0.557	0.165	0.401	0.566
0.5	(case 1b, case 2a)	0.591	0.168	0.410	0.578
2.5	(case 1b, case 2b)	0.912	0.224	0.577	0.801
3.5	(case 1b, case 2b)	0.952	0.232	0.608	0.840
4.5	(case 1b, case 2b)	0.970	0.237	0.630	0.867

Next, we discuss the GDPR's impact on the firm's profit. If α is small so that the firm's revenue does not depend significantly on data, then the GDPR benefits the firm. This can be seen from Propositions 1 and 2: When $\alpha < 1/4$, both the equilibrium price and demand increase after the GDPR, hence so does the profit. As α becomes large, however, the price increase after the GDPR can be countered by the decrease in total demand after the GDPR, as discussed in Proposition 2, which can eventually make the firm worse off after the GDPR. Simply put, when the firm's revenue depends heavily on data, the GDPR has a limited demand expansion effect and moreover can lead to a large loss in the amount of data collected as consumers switch to opt-out purchase.

Proposition 3. *There is a threshold value $\alpha_2 \in [1/4, 17/8]$ such that the equilibrium profit is larger after the GDPR if $\alpha \leq \alpha_2$ but smaller after the GDPR if $\alpha \geq \alpha_2$, that is, $\Delta\pi^* = \tilde{\pi}^* - \hat{\pi}^* \geq 0$ if and only if $\alpha \leq \alpha_2$.*

In Table 5, we compare the equilibrium profits for various values of α . As shown in the table, the equilibrium profit is larger after the GDPR for all α that leads to case 1a equilibrium before the GDPR and case 2a equilibrium after the GDPR, but smaller for all α that leads to case 2b equilibrium after the GDPR. The threshold value at which $\Delta\pi^* = 0$ is $\alpha_2 \approx 0.399$.

An implication of Proposition 3 is that the GDPR can benefit digital businesses that earn revenue primarily from selling services, of which the main channel is demand expansion thanks to more effective privacy management. Examples of such usage-driven businesses include ride-hailing platforms such as Uber, Lyft, streaming services such as Netflix, Spotify, and, to some extent, online marketplaces such as Amazon and eBay. But the GDPR can hurt digital businesses whose revenue is in large part based on data. Such data-driven businesses include various navigation and weather apps and, to some extent, Google and Facebook whose main revenue source is advertising that leverages user data. For these firms, the GDPR's demand expansion effect is limited, but loss of data collected following the GDPR can be significant.

In view of the above result that the GDPR has a negative impact on profits when α is large, the firm can

respond to the GDPR by switching its revenue model from a more data-based one (larger α) to a less data-based one (smaller α). This is supported by a recent work by Cheyre et al. (2023). They study how app developers on the Apple App Store responded to Apple's ATT framework introduced in June 2020. To the extent that ATT limits collection and sharing of user data, its impact on app developers is comparable to the impact of the GDPR. Following the introduction of ATT, they find that app developers reduced the use of software development kits (SDKs) that rely on data-intensive advertising but increased the use of SDKs related to authorization and payment services. This can be viewed as an example of switching the revenue model mentioned above.

Then, how does consumer surplus change after the GDPR? As discussed previously, consumers with low privacy costs are likely to be worse off because of the higher price after the GDPR, but those with high privacy costs are likely to be better off thanks to better privacy management. In particular, all consumers with $c < x$ are worse off either because they drop out of the market or because they pay a higher price after the GDPR. On balance, the GDPR is more likely to increase consumer surplus when α is smaller for the following reasons. First, when α is small, the equilibrium price before the GDPR is already close to the monopoly level and, therefore, the price increase following the GDPR is limited. Second, as explained earlier, there is significant room for demand expansion when α is small. Thus, the GDPR's demand expansion effect is more likely to dominate the price effect for smaller values of α , which increases consumer surplus. As α increases, however, the price effect together with the reduced demand expansion effect imply that the GDPR can decrease consumer surplus. Once again, the implication is that the GDPR can benefit consumers in markets that are largely service based, but it can hurt consumers when data-based revenue is a significant part of digital business.

Combining the above discussions and Proposition 3, we can conclude that the GDPR's effect on total surplus is also similar to that on profit and consumer surplus because total surplus is the sum of profit and consumer surplus. That is, the GDPR can increase total surplus at low values of α , but it can decrease it when α is large. Thus, the GDPR's welfare-improving effect is more likely in usage-driven businesses while its welfare-reducing effect is more likely in data-driven businesses.

Proposition 4. *Comparing the equilibria before and after the GDPR, we find the following.*

- *There is a threshold value α_3 such that the equilibrium consumer surplus is larger after the GDPR if $\alpha \leq \alpha_3$ but smaller after the GDPR if $\alpha \geq \alpha_3$, that is, $\Delta CS^* = \tilde{CS}^* - \hat{CS}^* \geq 0$ if and only if $\alpha \leq \alpha_3$.*

Table 5. Comparison of Equilibrium Profits

α	Equilibrium pair	Profit before the GDPR	Profit after the GDPR
0	(case 1a, case 2a)	0.145	0.266
0.1	(case 1a, case 2a)	0.182	0.281
0.2	(case 1a, case 2a)	0.226	0.297
0.25	(case 1b, case 2a)	0.250	0.305
0.4	(case 1b, case 2a)	0.329	0.329
0.5	(case 1b, case 2a)	0.387	0.346
2.5	(case 1b, case 2b)	1.979	0.743
3.5	(case 1b, case 2b)	2.913	0.971
4.5	(case 1b, case 2b)	3.875	1.206

• There is a threshold value α_4 such that the equilibrium total surplus is larger after the GDPR if $\alpha \leq \alpha_4$ but smaller after the GDPR if $\alpha \geq \alpha_4$, that is, $\Delta TS^* = \widehat{TS}^* - \widetilde{TS}^* \geq 0$ if and only if $\alpha \leq \alpha_4$.

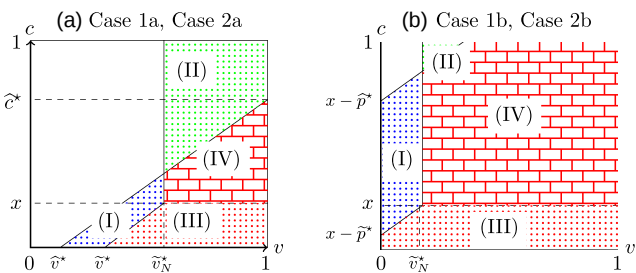
In Table 6, we compare the consumer surplus and total surplus for various values of α . The consumer surplus is larger after the GDPR when $\alpha < 0.2$ but smaller when $\alpha \geq 0.2$. The threshold value at which $\Delta CS^* = 0$ can be calculated as $\alpha_3 \approx 0.190$. Note that this threshold value is smaller than the threshold value for the GDPR's positive effect on profit, the latter being $\alpha_2 \approx 0.399$. This implies that the threshold value for the GDPR's positive effect on total surplus is between α_1 and α_3 . As shown in Table 6, the total surplus is larger after the GDPR when $\alpha < 0.4$ but smaller when $\alpha \geq 0.4$. Although not shown in the table, the threshold value at which $\Delta TS^* = 0$ can be calculated as $\alpha_4 \approx 0.333$.

We can explain the main mechanism behind the welfare impact of the GDPR with help of Figure 4, where $\widehat{v}^* = \widehat{p}^* - x$ and $\widehat{c}^* = 1 + x - \widehat{p}^*$ correspond to the equilibrium before the GDPR, and $\widetilde{v}^* = \widetilde{p}^* - x$ and $\widetilde{v}_N^* = \widetilde{p}^*$ correspond to the equilibrium after the GDPR. Because $\widetilde{p}^* > \widehat{p}^*$ as shown in Proposition 1, we have $\widetilde{v}^* < \widehat{v}^* < \widetilde{v}_N^*$. In Figure 4, four regions are labeled (I)–(IV) to indicate four groups of consumers choosing different behavior before and after the GDPR.

Figure 4(a) illustrates the case where α is relatively small; hence, the comparison is between case 1a equilibrium before the GDPR and case 2a equilibrium after the GDPR. Before the GDPR, the total equilibrium demand is represented by the triangle made up of (I), (III), and (IV). After the GDPR, the opt-out demand is the sum of areas (II) and (IV), and the opt-in demand is given by the trapezoid defined by the coordinates $(\widetilde{v}^*, 0)$, $(\widetilde{v}_N^*, x)$, $(1, 0)$, and $(1, x)$. Thus, the total demand after the GDPR is the sum of areas (II), (III), and (IV).

These changes in demand can be explained by considering the behavior of four groups of consumers. The first group is consumers in area (I), who drop out of the market after the GDPR because the firm raises its price after the GDPR. They have relatively low valuations

Figure 4. Comparison of Equilibrium Demands



Notes. (I) Consumers who drop out of the market after the GDPR. (II) Consumers who join the market through opt-out purchase after the GDPR. (III) Consumers who choose opt-in purchase both before and after the GDPR. (IV) Consumers who switch from opt-in purchase to opt-out purchase after the GDPR.

for the service and low privacy costs. Thus, the additional opt-out choice made available by the GDPR does not have much value for them. The second group is consumers in area (II), who buy the service only after the GDPR. They have relatively high valuations and high privacy costs. Because of high privacy costs, they do not buy the service before the GDPR but, after the GDPR, they choose opt-out purchase. The third group is consumers in area (III), who buy the service under both privacy regimes and share data as they have relatively low privacy costs ($c \leq x$). The fourth group is consumers in area (IV), who buy the service under both privacy regimes but choose opt-out purchase after the GDPR due to relatively high privacy costs ($c > x$). Thus, the GDPR creates winners and losers. The first and third groups of consumers are worse off after the GDPR. The second group of consumers is better off while the welfare change for the fourth group depends on the tradeoff between the higher price and better privacy management.

Figure 4(b), we consider the case where α is relatively large so that the comparison is between case 1b equilibrium before the GDPR and case 2b equilibrium after the GDPR. As before, the total equilibrium demand is the sum of areas (I), (III), and (IV) before the GDPR, and the sum of areas (II), (III), and (IV) after the GDPR. This

Table 6. Comparison of Consumer Surpluses and Total Surpluses

α	Equilibrium pair	Before the GDPR		After the GDPR	
		Consumer surplus	Total surplus	Consumer surplus	Total surplus
0	(case 1a, case 2a)	0.096	0.241	0.135	0.401
0.1	(case 1a, case 2a)	0.122	0.304	0.142	0.423
0.2	(case 1a, case 2a)	0.152	0.376	0.148	0.445
0.25	(case 1b, case 2a)	0.167	0.417	0.152	0.457
0.4	(case 1b, case 2a)	0.198	0.527	0.162	0.491
0.5	(case 1b, case 2a)	0.219	0.606	0.169	0.515
2.5	(case 1b, case 2b)	0.592	2.571	0.322	1.065
3.5	(case 1b, case 2b)	0.694	3.607	0.356	1.327
4.5	(case 1b, case 2b)	0.759	4.634	0.381	1.587

is the case where the market is sufficiently covered before the GDPR so that there is quite a small new demand created after the GDPR, that is, the area (II). But the price increase after the GDPR is sufficiently high so that consumers with high privacy costs and low valuations who purchased the service before the GDPR drop out of the market after the GDPR, that is, the area (I).³⁰

The general insight from the above discussions can be summarized with help of Table 7, where consumers are grouped based on (v, c) . The mass of consumers in each group is endogenous, as it depends on the equilibrium prices before and after the GDPR. The second column shows their choice before and after the GDPR and the last column shows the change in consumer surplus for each group, as explained above. For small values of α , that is, Figure 4(a), the pre-GDPR price is high, which implies that there is a large mass of consumers in group II, and their gains in consumer surplus outweigh the decrease in consumer surplus for groups I and III. Given the higher price and larger demand, profit also increases after the GDPR. This implies that total surplus increases after the GDPR when α is small. For large values of α , Figure 4(b), the pre-GDPR price is low, implying that the mass of consumers in group II is small, whereas those of other groups are significantly larger. Given that there are more consumers who lose after the GDPR (groups I and III) than those who gain (group II), total consumer surplus decreases after the GDPR. In addition, because a large mass of consumers in group I drop out of the market due to the price increase following the GDPR, profit also decreases after the GDPR. Put together, we can conclude that total surplus decreases when α is large.

6. Discussions and Extensions

6.1. Correlation Between v and c

Our baseline model assumed that v and c are independent. Depending on digital services, it is conceivable that there could be some correlations between the two. Take social media services, for example. A consumer who actively uses social media services may do so because she does not perceive the privacy cost to be high, which suggests a negative correlation between v and c .³¹ The correlation can be positive in medical services and health apps. These services often require users to share sensitive health data and therefore privacy-conscious individuals would choose to share such information as

they value these services highly. In this section, we allow correlations between v and c . In particular, we examine two polar cases of perfect positive and perfect negative correlations. The insight from these two cases may be used for extrapolation in intermediate cases.

6.1.1. Positive Correlation. Suppose $c = \phi v$ where $\phi \in (0, 1)$, and assume $x < \phi$ so that there is a positive mass of consumers who opt out after the GDPR, that is, consumers with $x < c = \phi v$, or $v > \tilde{v} := x/\phi$. In this case, the GDPR's demand expansion effect does not exist. The reason is that, given the perfect positive correlation, consumers who do not buy the service before the GDPR do not buy the service either after the GDPR. To see this, let $\hat{v}$ be the marginal consumer who buys the service before the GDPR, that is, $\hat{v} + (x - \phi\hat{v}) - p = 0$ and $[\hat{v}, 1]$ is the total demand before the GDPR. After the GDPR, the positive correlation between v and c implies that consumers on $[\hat{v}, \tilde{v}]$ continue to choose opt-in purchase, whereas those on $[\tilde{v}, 1]$ choose opt-out purchase. In addition, by the definition of $\tilde{v}$ and the fact that $\tilde{v} > \hat{v}$, no consumers outside $[\hat{v}, 1]$ participate in the market through opt-out purchase.

Consequently, the GDPR does not boost demand; it only divides the pre-GDPR total demand into opt-in and opt-out demands. As a result, the equilibrium price does not change after the GDPR. Given that the equilibrium price and total demand do not change, the firm is worse off after the GDPR. It is because the firm earns data-based revenue only from the opt-in demand after the GDPR, which is smaller than the total demand because consumers on $[\tilde{v}, 1]$ choose opt-out purchase after the GDPR. Finally, consumer surplus increases after the GDPR because the price stays the same while those choosing opt-out purchase benefit from privacy management. To summarize, the GDPR can hurt the firm and benefit consumers when v and c are positively correlated. It is worth noting that these results hold regardless of α .

6.1.2. Negative Correlation. Suppose now $c = 1 - \phi v$, where we set $\phi = 1$ to simplify analysis. Then, there is a positive mass of consumers who opt out after the GDPR because $x > 0$. Let $\tilde{v} = 1 - x$ be the marginal consumer, who is indifferent between opt-in purchase and opt-out purchase if $\tilde{v} \geq p$. Then, for all $v < \tilde{v}$, we have $c = 1 - v > 1 - \tilde{v} = x$. It follows that all consumers on $[p, \tilde{v}]$ choose opt-out purchase. That is, the negative

Table 7. Consumers' Choice Before and After the GDPR

Consumer types	Choice before and after the GDPR	ΔCS
Group I: (low to intermediate c , low v)	Opt-in purchase $\rightarrow$ no purchase	(-)
Group II: (high c , high v)	No purchase $\rightarrow$ opt-out purchase	(+)
Group III: (low c , low to high v)	Opt-in purchase $\rightarrow$ opt-in purchase	(-)
Group IV: (intermediate c , high v)	Opt-in purchase $\rightarrow$ opt-out purchase	(?)

correlation between v and c implies that consumers who choose opt-out purchase are those with lower valuations, hence higher privacy costs, than $\tilde{v}$, which is in contrast to the case with positive correlation. This implies that the GDPR can expand demand by inducing participation by consumers with low valuations who would not have opted in before the GDPR. More specifically, since consumers with low valuations choose opt-out purchase, the total demand after the GDPR is given by $D(p) = 1 - p$, which is independent of x . On the other hand, the demand before the GDPR increases in x . Thus, the GDPR's demand expansion effect depends on x : The GDPR is more likely to expand demand when x is smaller and decrease it when x is larger. To summarize, when v and c are negatively correlated, the GDPR's welfare effects depend on x and α , in contrast to the case with positive correlation.

Proposition 5. *Suppose v and c have a perfect positive correlation given by $c = \phi v$, $\phi > x$, $\phi \in (0, 1)$ and assume $\alpha < 1 + x - \phi$, which ensures that the equilibrium price is positive. Then, comparing the equilibria before and after the GDPR:*

- The price and demand are the same.
- The firm's profit is smaller but the consumer surplus is larger after the GDPR.

Suppose v and c have a perfect negative correlation given by $c = 1 - v$ and assume $\alpha < 1 + x$ which ensures that the equilibrium price is positive. Then, comparing the equilibria before and after the GDPR,

- The price is higher after the GDPR if and only if $\alpha > x$.
- The total demand is larger after the GDPR if and only if $\alpha < 1 - x$.
- There are threshold values α_L and α_H with $\alpha_L < \alpha_H$ such that the profit is larger after the GDPR if and only if $\max\{0, \alpha_L\} < \alpha < \min\{\alpha_H, 1 + x\}$.
- There is a threshold value α_{CS} such that the consumer surplus is larger after the GDPR if and only if $\alpha < \min\{\alpha_{CS}, 1 + x\}$.

Proof. See the Online Appendix.

6.2. When the Expected Privacy Cost Increases in α

Our baseline model assumed that a type (v, c) consumer incurs the privacy cost c when sharing data with the firm independent of α , that is, the firm's revenue model. Our interpretation is that c represents the consumer's maximum possible privacy cost, which the consumer expects to be equal to her actual privacy cost. We now consider an alternative scenario in which the consumer expects her actual privacy cost to vary depending on the firm's revenue model. Specifically, we assume that the expected privacy cost is a fraction of the maximum privacy cost with the fraction increasing in α .³² For example, the larger α is, the more data the firm collects, which may lead to larger expected costs from privacy breach. Although our model does

not allow different amounts of data that can be collected by the firm, we nonetheless consider the possibility that the expected privacy cost is higher when the firm's business model is more data driven.

Suppose a type (v, c) consumer's expected privacy cost is given by $f(\alpha)c$, where f is an increasing function of α . We assume $f(0) > 0$ so that the expected privacy cost from data sharing is positive even if the firm's business model is purely usage driven.³³ We also assume f is bounded above by one because the expected privacy cost cannot exceed the maximum possible privacy cost. Given this, a type (v, c) consumer's utility from opt-in purchase at price p changes from $U_S(v, c) = v + x - c - p$ to $U_S(v, c) = v + x - f(\alpha)c - p$. The rest of the baseline model remains the same.

In the following, we consider the case where f is given by $f(\alpha) = k + (1 - k)\alpha$ for some $k \leq 1$ and focus on the case with $x = 1/4$ and $\alpha \in [0, 1]$.³⁴ We restrict the value of k such that $f(\alpha)c > x$. This is to rule out the trivial case where all consumers choose opt-in purchase, in which case the GDPR does not have any impact. Because $f(\alpha) = 1$ when $k = 1$, our baseline model corresponds to the case where $k = 1$. Thus, when $k = 1$, our results that the GDPR decreases the equilibrium profit and consumer surplus stay the same. For all other values of $k < 1$, we have $f(\alpha) < 1$, hence the expected privacy cost $f(\alpha)c$ is less than c . In addition, $f(\alpha)c$ decreases as k decreases, which implies that the benefits of GDPR decrease because there is less value in privacy management when the expected privacy cost is lower. Thus, as k decreases, we expect the threshold values of α at which the GDPR increases profit or consumer surplus to become smaller.

To verify the above, we solve the model for the equilibria before and after the GDPR when $U_S(v, c) = v + x - (k + (1 - k)\alpha)c - p$, calculate the equilibrium profits and consumer surpluses, and find the relevant threshold values of α . The results are shown in Table 8 with full analysis provided in the Online Appendix. In the second column, we calculate the threshold values of α at which the GDPR's effect on the equilibrium profit is zero, that is, $\Delta\pi^* = \tilde{\pi}^* - \hat{\pi}^* = 0$, as discussed in Proposition 3. The GDPR increases the equilibrium profit if and only if α is below this threshold, as in our baseline model. The third column shows the threshold values of

Table 8. When the Expected Privacy Cost Increases in α

k	Value of α when $\Delta\pi^* = 0$	Value of α when $\Delta CS^* = 0$
0.4	0.128	0.053
0.5	0.190	0.083
0.6	0.243	0.108
0.7	0.288	0.128
0.8	0.329	0.144
0.9	0.366	0.155
1.0	0.399	0.191

α at which the GDPR's effect on the equilibrium consumer surplus is zero, that is, $\Delta CS^* = \widetilde{CS}^* - \widehat{CS}^* = 0$, as discussed in Proposition 4. The GDPR increases the equilibrium consumer surplus if and only if α is below this threshold, as in our baseline model.

The main difference between the results in this section and our baseline model is that the relevant threshold values of α are smaller than those in the baseline model, and they decrease as k decreases, as shown in Table 8. Thus, a positive relation between α and the expected privacy costs dampens the welfare effects of the GDPR. This is not surprising in that our baseline model assumed that consumers expect the actual privacy costs to be equal to the maximum possible privacy costs; hence, the GDPR's privacy management has more benefits than what was considered in this section. Nonetheless, our main insight continues to hold that the GDPR can be welfare improving for small values of α but can reduce welfare for large values of α .

6.3. Data Externalities

A consumer's data-sharing decision can impose several types of externalities on others. First, consumers using the firm's service may enjoy network benefits that increase as more consumers share data with the firm (Hagiu and Wright 2023). For example, online retailers such as Amazon and Etsy rely on various user-generated data including product reviews and ratings to provide valuable information to consumers. Network benefits may also include improved products and services that sellers on the marketplaces can provide based on customer feedback. Second, data sharing by some consumers can impose negative externalities in the form of larger privacy costs on others who do not share data (Choi et al. 2019, Ichihashi 2021, Bergemann et al. 2022, Miklós-Thal et al. 2024). For example, some people's shared data can be used to infer information about others who do not share data. As more data are shared, the inference can be improved through machine learning, which leads to larger privacy costs. As another example, hackers can use personal data obtained from one group of users to craft convincing phishing emails or other social engineering attacks targeted at another group of users. Third, there can be negative pecuniary externalities whereby the firm can use the data on opt-in consumers to infer information on and charge higher price to opt-out consumers (Belleflamme and Vergote 2016, Braghieri 2017). In this section, we consider the first two, positive network benefits and negative data externalities, and discuss how our main results may change.

6.3.1. Positive Network Benefits. As discussed above, we consider positive network benefits that increases in the mass of opt-in consumers. Denote network benefits by θD_S where $\theta \geq 0$ is an exogenously given value accruing from an additional opt-in consumer. We assume that

network benefits are enjoyed by all consumers who buy the service whether they share data with the firm. For example, even if a consumer makes a purchase at an online shop without creating an account, she can still read all the reviews and ratings. Thus, the main difference between opt-in and opt-out purchase is that a consumer choosing opt-in purchase expects additional opt-in benefits as well as privacy costs, which is the same as in the baseline model.

When there are network benefits, a consumer's opt-in decision depends on her expectation on the mass of opt-in consumers, which we denote by D_S^e . Then, a consumer of type (v, c) derives expected utility

$$U(v, c, D_S^e) = \begin{cases} U_S := v + (x - c) + \theta D_S^e - p, & \text{with opt-in purchase,} \\ U_N := v + \theta D_S^e - p, & \text{with opt-out purchase,} \\ U_O := 0, & \text{without purchase.} \end{cases}$$

As is clear from the above, consumers are more likely to purchase the service because both $U_S - U_O$ and $U_N - U_O$ increase by θD_S^e compared with the case without network benefits. But network benefits do not affect their opt-in decisions because $U_S - U_N$ is the same with or without network benefits. Given that the GDPR's main effect in our model is to allow consumers to make opt-in decisions proactively, we expect our key insight from the baseline model to remain unchanged.

6.3.2. Negative Data Externalities. Suppose negative data externalities are proportionate to the consumer's privacy cost and the expected mass of opt-in consumers, D_S^e . Let $\gamma \geq 0$ represent the magnitude of negative externalities, so that consumer (v, c) suffers total negative externalities equal to $\gamma c D_S^e$. We can consider two possible ways negative externalities can be introduced to the baseline model. First, suppose negative externalities affect all consumers including those who share data, as in Choi et al. (2019). In this case, all consumers' utility decreases by $\gamma c D_S^e$, whether they choose opt-in purchase, opt-out purchase, or no purchase. Consequently, the analysis is exactly the same as before.

Suppose now that negative externalities affect consumers who do not share data, whether they buy the service. Then, consumer (v, c) derives utility

$$U(v, c, D_S^e) = \begin{cases} U_S := v + (x - c) - p, & \text{with opt-in purchase,} \\ U_N := v - \gamma c D_S^e - p, & \text{with opt-out purchase,} \\ U_O := -\gamma c D_S^e, & \text{without purchase.} \end{cases}$$

As is clear from the above, negative externalities make opt-in a more attractive choice than opt-out: compared with the baseline model, $U_S - U_N$ increases by $\gamma c D_S^e$. In addition, $U_S - U_O$ also increases by $\gamma c D_S^e$ but $U_N - U_O$

stays the same. Put together, we can conclude that negative externalities increase the proportion of consumers who choose opt-in purchase. This diminishes the value of an option to choose opt-out purchase, which dampens the effect of the GDPR. But our key insight does not change because the main mechanism that the GDPR can create more demand remains intact even in the presence of negative externalities. That is, the GDPR allows consumers with large privacy costs who stay out of the market before the GDPR to participate in the market through opt-out purchase; negative externalities reduce, but not eliminate, the proportion of such consumers. In addition, by making opt-in a more attractive choice than opt-out, negative externalities also reduce the proportion of consumers who exit the market after the GDPR because of the high price.

6.4. When Consumers Differ Only in Valuations of the Service

One of our key results is how the GDPR leads to a substitution between data quantity and the value of data as summarized in Proposition 2, that is, $\tilde{D}_S^* < \hat{D}^*$ but $\tilde{v}^* > \hat{v}^*$. This result depends crucially on consumer heterogeneity in privacy costs. To verify this claim, we briefly discuss the case without consumer heterogeneity in privacy costs. Suppose c is constant and denote $z := x - c$ so that consumer type is represented by v only.

Before the GDPR, consumer v buys the service if $v \geq p - z$; hence, $D = 1 - (p - z)$. Maximizing $\Pi = (p + \alpha)D$ gives us $\hat{p}^* = (1 + z - \alpha)/2$ and $\hat{D}^* = (1 + z + \alpha)/2$. After the GDPR, we have two cases. First, if $z \geq 0$, then there is only opt-in purchase, implying that the outcome is the same as that before the GDPR. In this case, the GDPR has no effect on the amount of data shared. Second, if $z < 0$, then there is only opt-out purchase. Then $D = D_N = 1 - p$ and $D_S = 0$. Maximizing $\Pi = pD + \alpha D_S$ leads to $\tilde{p}^* = \tilde{D}^* = 1/2$ and $\tilde{D}_S^* = 0$.

Comparing the above and noting that $z < 0$ in this case, we find $\tilde{p}^* > \hat{p}^*$ always holds and $\tilde{D}^* > \hat{D}^*$ if and only if $\alpha + z < 0$. That is, the equilibrium price increases after the GDPR, and the equilibrium demand increases if and only if $\alpha < c - x$. It is also straightforward to check that the equilibrium profit increases after the GDPR if and only if $\alpha < c - x$. But the quantity of shared data either does not change or decreases to zero. Thus, there is no possibility that the GDPR reduces the quantity of data while increasing the marginal consumer's valuation for the firm's service. This is intuitively clear because, in the absence of consumer heterogeneity in privacy costs, there is no sense in which the GDPR can invite consumers with high privacy costs to choose opt-out purchase.

6.5. Testable Hypotheses

In this section, we summarize testable hypotheses that can be derived from our analysis and discuss the issues relevant to testing these hypotheses.

Our main hypotheses can be summarized as follows. First, for digital businesses whose main revenue source is selling services, empowering consumers to make informed and proactive decisions for data sharing can increase price for the service, consumer activity, business profitability, and consumer surplus. Second, for digital businesses whose main revenue source is data that are collected through selling services, more effective privacy management by consumers can increase price for the service but decrease consumer activity, business profitability, and consumer surplus. As discussed earlier, the examples of usage-driven businesses include various ride-hailing platforms and streaming services and, to some extent, online marketplaces, whereas data-driven businesses include various navigation and weather apps and, to some extent, digital platforms whose main revenue source is advertising that leverages user data.

There is an important caveat in testing the above hypotheses. Our model assumes fully informed consumers who can rationally choose between opt-in and opt-out purchase after the introduction of new privacy regulations, the GDPR being the focus of our paper. However, one may argue that, even after the GDPR, consumers' ability to manage privacy may be hampered for various reasons. First, the GDPR's cookie rules are not refined enough, which has led to a proliferation of diverse consent management platforms and failed to enable consumers to effectively manage their privacy (Chen 2022, Chaudhury and Choe 2023). Second, many websites continue to rely on dark patterns, implied consent, and various forms of nudging to influence consumers' data-sharing decisions (Utz et al. 2019, Machuletz and Böhme 2020, Matte et al. 2020, Nouwens et al. 2020). Third, consumers generally show apathy toward complex and long privacy notices and select the "quick join" clickwrap to gain access to a website (Obar and Oeldorf-Hirsch 2020).

In view of the above issues, the GDPR's welfare implications analyzed in this study need to be understood to apply to an environment where the GDPR achieves its stated purpose of enabling consumers to make an informed and unambiguous consent to data sharing. However, identifying GDPR-compliant consent management platforms that are quarantined from the above compounding factors can be challenging. It can also lead to a selection bias. Therefore, our hypotheses may be best tested in carefully designed experiments.

6.6. Implications for Management

Our analysis generates at least three clear implications for management relevant to digital businesses with some market power. First, empowering customers in privacy management can benefit the business that does not rely heavily on data-based revenue. As we have shown, active privacy management can expand demand

as privacy-conscious consumers can choose from multiple options to buy the service. This allows the business to raise price if it has some market power. The implication is that, even in jurisdictions without the GDPR-type opt-in requirements, businesses may consider proactively empowering customers in privacy management. After all, today's savvy consumers can, with a little research, find the information they need to make informed decisions. Providing them upfront with clear information and available options can also minimize potential backlash and reduce customer churn.

Second, we identified potential conflicts between usage-based revenue and data-based revenue. As the size of data-based revenue grows, the business has an incentive to lower prices to attract more consumers and hence more data. This can erode the usage-based revenue. One possible way to manage such conflicts is to separate the two revenue sources into independent businesses. For example, a firm that provides advertising services can have a separate entity responsible for collecting and monetizing user data. Of course, this is subject to usual considerations relevant to corporate restructuring.³⁵ The establishment of Alphabet in 2015 may be understood in this context. Alphabet was formed as a holding company that oversees several separate businesses including Google. This separation allowed Google to focus on its core search and advertising business while giving other Alphabet subsidiaries such as Life Sciences and Calico greater autonomy to pursue their own initiatives.³⁶ Another example involves Twitter and Gnip, an independent social media API aggregation company. Twitter had a data licensing agreement with Gnip in 2010 for selling access to Twitter's data to other companies. This allowed Twitter to focus on its core business of providing a social media platform while giving Gnip the freedom to focus on monetizing Twitter's data.³⁷

Finally, our analysis suggests how online businesses with data-based revenue model can respond to privacy regulations such as the GDPR in order to blunt the negative impact of the regulation. The key takeaway is that they need to reduce the reliance on data as the main revenue source and explore other revenue sources such as paid subscriptions. We have already mentioned Cheyre et al. (2023), who show how app developers responded to Apple's ATT by reducing the use of SDKs that rely on advertising and increasing the use of SDKs related to payment services. Other examples include Meta and X (formerly Twitter). Facebook and Instagram (owned by Meta) launched a paid subscription service in 2023 in a bid to remove ads from the platforms.³⁸ X has also introduced a three-tiered paid premium subscription service to expand its revenue sources.³⁹

7. Conclusion

This paper studied the GDPR's opt-in requirement in a simple model with a monopolistic firm and consumers

who differ in both valuations of the firm's service and privacy costs. The firm's revenue comes from two sources: sales of its service that we call usage-based revenue and monetization of data that we call data-based revenue. Our basic assumption is that consumers can choose to buy the service without sharing data, called opt-out purchase, only after the GDPR. Relaxing this assumption will not alter our main insight, as long as more consumers proactively manage their privacy after the GDPR, the latter supported by various empirical and experimental studies.

We showed that the GDPR expands demand for the firm's service by inviting consumers with high privacy costs to participate in the market through opt-out purchase. This allows the firm to raise prices for its service. If the firm's revenue is largely usage based, then the equilibrium demand also increases despite the higher price. In this case, the firm benefits from the GDPR because of the higher price and larger demand. Consumer surplus also increases mainly due to the increased consumer participation in the market through privacy management. On the other hand, some consumers with high privacy costs and high valuations who bought the service before the GDPR can switch to opt-out purchase after the GDPR. This leads to a smaller quantity of shared data, which erodes the firm's data-based revenue. Thus, the firm's profit can decrease after the GDPR if its revenue is largely data based. Moreover, the higher price after the GDPR can lead some consumers with low valuations to drop out of the market after the GDPR, decreasing consumer surplus as a result. Put together, we conclude that the GDPR has differing effects on the firm and consumers, depending on the firm's revenue structure. For a firm without significant data-based revenue, the GDPR can increase profits and consumer surplus and hence can be welfare improving. But it can decrease welfare when data-based revenue is significant for the firm.

Although the main focus of our paper has been on the GDPR, our model can be applied more broadly to situations where consumers differ in their privacy preferences. Such heterogeneity may motivate firms to cater to different groups of consumers by offering different versions of their services, the simplest example being a binary choice between opt-in and opt-out purchase studied in this paper. Although the current paper has not provided general analysis of such a versioning strategy, the analytical framework for this is similar to that used in the studies on ad avoidance (Anderson and Gans 2011, Lin 2020, Amaldoss et al. 2024). In these studies, firms offer different versions of digital content depending on the number of ads consumers are exposed to when consuming the content. Such an offer is credible because consumers can directly verify their exposure to ads. In contrast, the credibility of an offer of opt-out choice in our paper needs a commitment

device such as the GDPR because consumers cannot tell whether their data are shared unless the cost of data breach is realized. We leave the study of versioning strategies given consumers' heterogeneous privacy preferences for future research.⁴⁰

Acknowledgments

Author names are alphabetically ordered. All authors contributed equally. The authors thank the department editor for the thoughtful review process; the associate editor and anonymous reviewers for many valuable comments and suggestions; and Cédric Argenton, Anastasios Dosis, Joshua Gans, Clara Graziano, Claudia Herresthal, Hooman Hidaji, Ulrich Laitenberger, Melika Liporace, Keizo Mizuno, Andrea Mantovani, Barry R. Nault, Jens Prüfer, Markus Reisinger, Susumu Sato, Florian Schuett, Radosława Shopova, Tat-How Teh, Mark Tremblay, Vaarun Vijairaghavan, Chengsi Wang, and participants at numerous conferences, seminars, and workshops for helpful comments. The usual disclaimer applies.

Appendix

This appendix presents analysis of the model for general values of x and α . Missing proofs are all relegated to an Online Appendix. The results presented in Sections 4 and 5 can be reproduced by substituting $x = 1/4$ into the results provided below.

A.1. Equilibrium Before the GDPR

The firm chooses $\hat{p}$ to maximize $\hat{\Pi}(\hat{p}) = (\hat{p} + \alpha)\hat{D}(\hat{p})$ where $\hat{D}(\hat{p})$ is given in (4). Solving the first-order condition for $\hat{p}$, we obtain⁴¹

$$\hat{p}^* = \begin{cases} \frac{1+x-2\alpha}{3} & \text{if } x < \hat{p}^* < 1+x, \\ \frac{2(x-1)-\alpha + \sqrt{6+(x+\alpha-1)^2}}{3} & \text{if } x-1 < \hat{p}^* \leq x. \end{cases}$$

In the first case, one can verify that $\hat{p}^* > x$ if and only if $\alpha < \alpha_1(x)$ and $\hat{p}^* < 1+x$ always holds, where

$$\alpha_1(x) := \max\left\{\frac{1-2x}{2}, 0\right\}.$$

In the second case, we have $\hat{p}^* \leq x$ if and only if $\alpha \geq \alpha_1(x)$ and $\hat{p}^* > x-1$ always holds. In addition, given $\alpha \geq 0$, both cases are possible if $(1-2x)/2 \geq 0$ or $x \leq 1/2$; otherwise, only case 1b is possible.

Substituting $\hat{p}^*$ into the demand, we obtain the equilibrium price and demand as

$$(\hat{p}^*, \hat{D}^*) = \begin{cases} \left(\frac{1+x-2\alpha}{3}, \frac{2(1+x+\alpha)^2}{9}\right) & \text{if } \alpha < \alpha_1(x), \\ \left(\frac{2(x-1)-\alpha+\beta}{3}, \frac{6-(x+\alpha-1)^2+\beta(x+\alpha-1)}{9}\right) & \text{if } \alpha \geq \alpha_1(x), \end{cases}$$

where $\beta := \sqrt{6+(x+\alpha-1)^2}$. The corresponding profit is $\hat{\Pi}^*$

$= (\hat{p}^* + \alpha)\hat{D}^*(\hat{p}^*)$, and consumer surplus is $\widehat{CS}^*$ is given by

$$\widehat{CS}^*(\hat{p}^*) = \begin{cases} \int_{v(\hat{p}^*)}^1 \int_0^{c(v,\hat{p}^*)} U_S(v,c) dc dv & \text{if } \alpha < \alpha_1(x), \\ \int_0^{1+v(\hat{p}^*)} \int_0^{c(v,\hat{p}^*)} U_S(v,c) dc dv & \text{if } \alpha \geq \alpha_1(x). \end{cases}$$

Thus, we have

$$\hat{\Pi}^* = \begin{cases} \hat{\Pi}_{1a}^* = \frac{2(1+x+\alpha)^3}{27} & \text{if } \alpha < \alpha_1(x), \\ \hat{\Pi}_{1b}^* = \frac{(2(x+\alpha-1)+\beta)(6-(x+\alpha-1)^2+\beta(x+\alpha-1))}{27} & \text{if } \alpha \geq \alpha_1(x). \end{cases}$$

$$\widehat{CS}^* = \begin{cases} \widehat{CS}_{1a}^* = \frac{4(1+x+\alpha)^3}{81} & \text{if } \alpha < \alpha_1(x), \\ \widehat{CS}_{1b}^* = \frac{81+18(x+\alpha-1)-2(x+\alpha-1)^3-2\beta(12-(x+\alpha-1)^2)}{81} & \text{if } \alpha \geq \alpha_1(x). \end{cases}$$

The following lemma provides the comparative statics of the above equilibrium outcome.

Lemma A.1. *The equilibrium price increases in the opt-in benefits x and decreases in the marginal data-based revenue α . The equilibrium demand, profit, and consumer surplus are all increasing in x and α .*

When $x = 1/4$ as assumed in the main text, we have $\alpha_1(x) = 1/4$. Then, Lemma 1 is obtained by substituting $x = 1/4$ into the above expressions.

A.2. Equilibrium After the GDPR

The firm chooses $\tilde{p}$ to maximize $\tilde{\Pi}(\tilde{p}) = \tilde{p}(\tilde{D}_S(\tilde{p}) + \tilde{D}_N(\tilde{p})) + \alpha\tilde{D}_S(\tilde{p})$, where $\tilde{D}_S(\tilde{p})$ and $\tilde{D}_N(\tilde{p})$ are as given in the main text. Solving the firm's problem, we obtain $\tilde{p}^* = (2-2\alpha x+x^2)/4$ if $x < \tilde{p}^* \leq 1$ and $\tilde{p}^* = (\Gamma-2-\alpha+2x)/3$ if $0 < \tilde{p}^* \leq x$, where $\Gamma := \sqrt{6+(2-2x+\alpha)^2}$. In the first case, one can verify that $\tilde{p}^* \leq 1$ always holds and $\tilde{p}^* > x$ if and only if $\alpha < \alpha_2(x)$, where

$$\alpha_2(x) := \max\left\{\frac{2-4x+x^2}{2x}, 0\right\}.$$

In the second case, we have $\tilde{p}^* \leq x$ if and only if $\alpha \geq \alpha_2(x)$ and $\tilde{p}^* > 0$ always holds. Also, given $\alpha \geq 0$, both cases are possible if $(2-4x+x^2)/(2x) \geq 0$ or $x \leq 2-\sqrt{2} \approx 0.585$; otherwise, only case 2b is possible. Put together, we can write the equilibrium price after the GDPR as⁴²

$$\tilde{p}^* = \begin{cases} \frac{2(1-\alpha x)+x^2}{4} & \text{if } \alpha < \alpha_2(x), \\ \frac{\Gamma-(2-2x+\alpha)}{3} & \text{if } \alpha \geq \alpha_2(x). \end{cases}$$

Substituting $\tilde{p}^*$ into the opt-in demand, we obtain

$$\tilde{D}_S^* = \begin{cases} \frac{x(2+2\alpha x+2x-x^2)}{4} & \text{if } \alpha < \alpha_2(x), \\ x - \frac{3+(2-2x+\alpha)^2-\Gamma(2-2x+\alpha)}{9} & \text{if } \alpha \geq \alpha_2(x). \end{cases}$$

Similarly, the opt-out and total demands can be calculated as

$$(\tilde{D}_N^*, \tilde{D}^*) = \begin{cases} \left(\frac{(1-x)(2+2\alpha-x^2)}{4}, \frac{2+2\alpha+x^2}{4} \right) & \text{if } \alpha < \alpha_2(x), \\ \left(\frac{(1-x)(5+\alpha-2x-\Gamma)}{3}, \frac{6-(2+\alpha-2x-\Gamma)(x+\alpha-1)}{9} \right) & \text{if } \alpha \geq \alpha_2(x). \end{cases}$$

Then, the firm's profit $\tilde{\Pi}^*$ and consumer surplus $\tilde{CS}^*$ are given by

$$\tilde{\Pi}^* = \begin{cases} \tilde{\Pi}_{2a}^* = \frac{4+4x(x+2\alpha+2\alpha x)+x^2(x-2\alpha)^2}{16}, & \text{if } \alpha < \alpha_2(x), \\ \tilde{\Pi}_{2b}^* = \frac{-27(2-\alpha x)+36(1+2x-\alpha)-9(1+2x-\alpha)^2+(1+2x-\alpha)^3}{27} \\ \quad + \frac{\Gamma(15-(5-2x+\alpha)(1+2x-\alpha))}{27} & \text{if } \alpha \geq \alpha_2(x), \end{cases}$$

$$\tilde{CS}^* = \begin{cases} \tilde{CS}_{2a}^* = \frac{12+24\alpha x+12(1+\alpha^2)x^2+4(4+3\alpha)x^3-9x^4}{96} & \text{if } \alpha < \alpha_2(x), \\ \tilde{CS}_{2b}^* = \frac{\delta(\delta^2-9x\delta+27x^2)-9(10-4x+3x^2+2\alpha)\delta+27(5+3x^2)}{162} & \text{if } \alpha \geq \alpha_2(x), \end{cases}$$

where $\delta := \Gamma - (2 - 2x + \alpha)$.

The following lemma provides the comparative statics of the above equilibrium outcome.

Lemma A.2. *The equilibrium price decreases in x if and only if $\alpha_2(x) > \alpha \geq x$. The equilibrium price decreases in α . Both the equilibrium opt-in demand and total demand increase in x and α . The equilibrium opt-out demand increases in x if and only if $\alpha_2(x) > \alpha > \alpha_3(x) := \frac{2+2x-3x^2}{2-4x}$, and always increases in α . Both the equilibrium profit and consumer surplus increase in x and α .*

When $x = 1/4$, we have $\alpha_2(x) = 17/8$. Then, Lemma 2 is obtained by substituting $x = 1/4$ into the above expressions.

A.3. Comparing the Equilibria Before and After the GDPR

Our analysis in the previous section shows that different equilibria exist for different values of (x, α) . Before the GDPR, we have case 1a equilibrium if $\alpha \leq \alpha_1(x)$ and case 1b equilibrium if $\alpha > \alpha_1(x)$ where $\alpha_1(x)$ is given in (7). Because $\alpha \geq 0$, case 1a equilibrium exists only if $x \leq 1/2$ because $\alpha_1(x) = 0$ if $x > 1/2$. This implies that case 1a equilibrium exists for $(x, \alpha) \in \{(x, \alpha) | \alpha \leq \alpha_1(x), x \leq 1/2\}$, and case 1b equilibrium exists for $(x, \alpha) \in \{(x, \alpha) | \alpha > \alpha_1(x), x \leq 1/2\}$ or $(x, \alpha) \in \{(x, \alpha) | \alpha > \alpha_1(x), x > 1/2\}$. Applying a similar argument to the case after the GDPR, we can conclude that case 2a equilibrium exists for $(x, \alpha) \in \{(x, \alpha) | \alpha \leq \alpha_2(x), x \leq 2 - \sqrt{2}\}$ and case 2b equilibrium exists for $(x, \alpha) \in \{(x, \alpha) | \alpha > \alpha_2(x)\}$, where $\alpha_2(x)$ is given in (7). In addition, we can verify $\alpha_2(x) \geq \alpha_1(x)$, which implies that we cannot have case 1a equilibrium before the GDPR co-existing with case 2b equilibrium after the GDPR. Based on these discussions, we can identify a pair of equilibria corresponding to all possible values of (x, α) , which we summarize below.

Lemma A.3. *A pair of equilibria before and after the GDPR can be fully described as follows:*

- If $x \leq 1/2$ and $\alpha < \alpha_1(x)$, then we have case 1a equilibrium before the GDPR and case 2a equilibrium after the GDPR.
- If $x \leq 2 - \sqrt{2}$ and $\alpha_1(x) \leq \alpha < \alpha_2(x)$, then we have case 1b equilibrium before the GDPR and case 2a equilibrium after the GDPR.
- If $x \leq 1$ and $\alpha \geq \alpha_2(x)$, then we have case 1b equilibrium before the GDPR and case 2b equilibrium after the GDPR.

Proof. From the preceding discussions, we can identify three possible pairs of equilibria as follows. First, if $x \leq 1/2$, then we have (case 1a equilibrium, case 2a equilibrium) if $\alpha < \alpha_1(x) \leq \alpha_2(x)$, (case 1b equilibrium, case 2a equilibrium) if $\alpha_1(x) \leq \alpha < \alpha_2(x)$, and (case 1b equilibrium, case 2b equilibrium) if $\alpha_1(x) \leq \alpha_2(x) \leq \alpha$. Second, if $1/2 < x \leq 2 - \sqrt{2}$, then we have (case 1b equilibrium, case 2a equilibrium) if $\alpha < \alpha_2(x)$, and (case 1b equilibrium, case 2b equilibrium) if $\alpha \geq \alpha_2(x)$. Third, if $2 - \sqrt{2} < x \leq 1$, then we have (case 1b equilibrium, case 2b equilibrium) for all α . The lemma follows from this. $\square$

Comparing the above three pairs of equilibria, we can show the following.

Proposition A.1. *The equilibrium price is higher after the GDPR, that is, $\tilde{p}^* > \hat{p}^*$.*

Proposition A.2. *Comparing the equilibria before and after the GDPR, we find the following:*

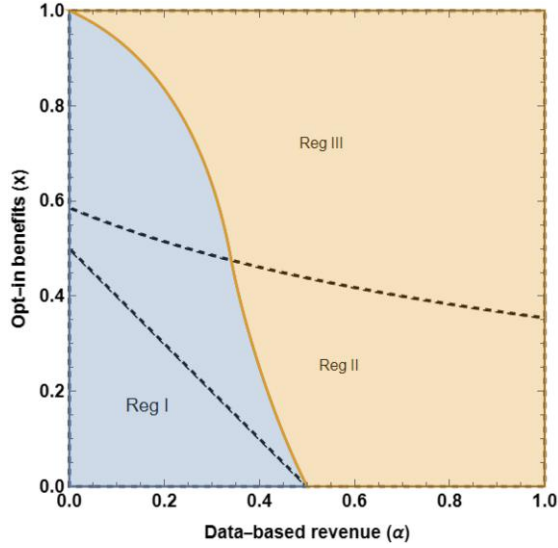
- When $\alpha < \alpha_1(x)$, the total demand is larger after the GDPR, i.e., $\tilde{D}^* > \hat{D}^*$.
- When $\alpha_1(x) \leq \alpha < \alpha_2(x)$, we have $\tilde{D}^* > \hat{D}^*$ if and only if $\alpha < \min\{\alpha_2(x), \alpha_4(x)\}$ where $\alpha_4(x)$ is the value of α that solves $4\beta(1-x-\alpha) + 4\alpha^2 + 26\alpha x + 13x^2 - 2 - 8(x+\alpha) = 0$ and $\beta = \sqrt{6 + (x+\alpha-1)^2}$.
- When $\alpha \geq \alpha_2(x)$, we have $\tilde{D}^* > \hat{D}^*$ if and only if $\alpha < 1 - x$.
- For all values of α , the opt-in demand after the GDPR is smaller than the total demand before the GDPR, that is, $\hat{D}^* > \tilde{D}_S^*$.
- The marginal consumer with lowest privacy cost who shares data has a higher valuation for the service after the GDPR: $\tilde{v}^* > \hat{v}^*$.

Proposition A.3. *Comparing the equilibria before and after the GDPR, we find the following:*

- When $\alpha < \alpha_1(x)$, the firm's profit is larger after the GDPR, that is, $\tilde{\Pi}_{2a}^* > \hat{\Pi}_{1a}^*$.
- When $\alpha_1(x) \leq \alpha < \alpha_2(x)$, we have $\tilde{\Pi}_{2a}^* > \hat{\Pi}_{1b}^*$ if and only if $\alpha \leq \min\{\alpha_2(x), \alpha_5(x)\}$ where $\alpha_5(x)$ is the value of α that solves $\tilde{\Pi}_{2a}^* = \hat{\Pi}_{1b}^*$.
- When $\alpha \geq \alpha_2(x)$, we have $\tilde{\Pi}_{2b}^* > \hat{\Pi}_{1b}^*$ if and only if $\alpha_2(x) < \alpha < \alpha_6(x)$ where $\alpha_6(x)$ is the value of α that solves $\tilde{\Pi}_{2b}^* = \hat{\Pi}_{1b}^*$.

Figure A.1 illustrates Proposition A.3. In the figure, the blue-shaded region labeled $\Delta\Pi > 0$ is where the firm's profit increases after the GDPR and the yellow-shaded region labeled $\Delta\Pi < 0$ is where the firm's profit decreases after the GDPR. The curved line dividing these two regions is defined by $\alpha_5(x)$ and $\alpha_6(x)$ stated in Proposition A.3. The two dashed lines divide the set of (α, x) into three regions. The region labeled Reg I corresponds to the case where $\alpha < \alpha_1(x)$, Reg 2 corresponds to the case where $\alpha_1(x) \leq \alpha < \alpha_2(x)$, and Reg 3 corresponds to the case where $\alpha \geq \alpha_2(x)$. As shown in the figure, for given values of x , the GDPR benefits the firm for smaller values of α

Figure A.1. Comparison of Equilibrium Profits:
 $\Delta\Pi = \hat{\Pi}^* - \hat{\Pi}^*$



but hurts the firm for larger values of α , with smaller values of x admitting a larger range of α that benefits the firm. It is because, the smaller x is, the larger is the mass of consumers who participate in the market through opt-out purchase after the GDPR, as can be checked in Figure A.1. This leads to a larger demand expansion effect.

Proposition A.4. Comparing the equilibria before and after the GDPR, we find the following:

- When $\alpha < \alpha_1(x)$, the consumer surplus is larger after the GDPR, that is, $\widehat{CS}_{2a}^* > \widehat{CS}_{1a}^*$, if and only if $\alpha < \alpha_7(x)$ where $\alpha_7(x)$ is the value of α that solves $\widehat{CS}_{2a}^* = \widehat{CS}_{1a}^*$.
- When $\alpha_1(x) \leq \alpha < \alpha_2(x)$, we have $\widehat{CS}_{2a}^* > \widehat{CS}_{1b}^*$ if and only if $\alpha < \alpha_8(x)$ where $\alpha_8(x)$ is the value of α that solves $\widehat{CS}_{2a}^* = \widehat{CS}_{1b}^*$.
- When $\alpha \geq \alpha_2(x)$, we have $\widehat{CS}_{2b}^* > \widehat{CS}_{1b}^*$ if and only if $\alpha < \alpha_9(x)$ where $\alpha_9(x)$ is the value of α that solves $\widehat{CS}_{2b}^* = \widehat{CS}_{1b}^*$.

Figure A.2. Comparison of Consumer Surpluses:
 $\Delta CS = \widehat{CS}^* - \widehat{CS}^*$

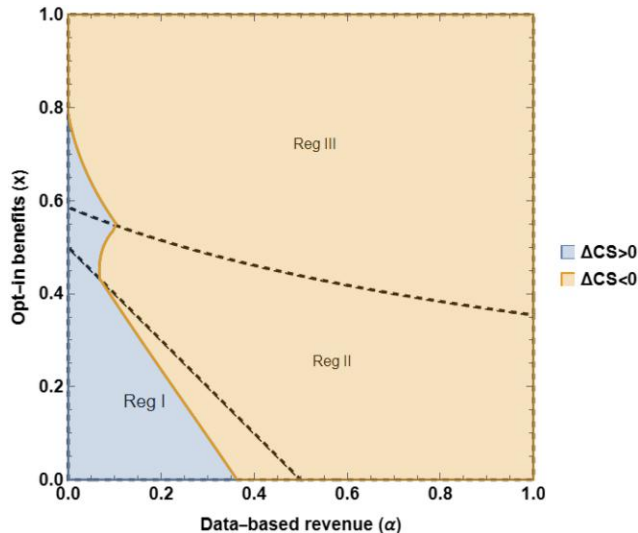


Figure A.3. Comparison of Consumer Surpluses and Profits

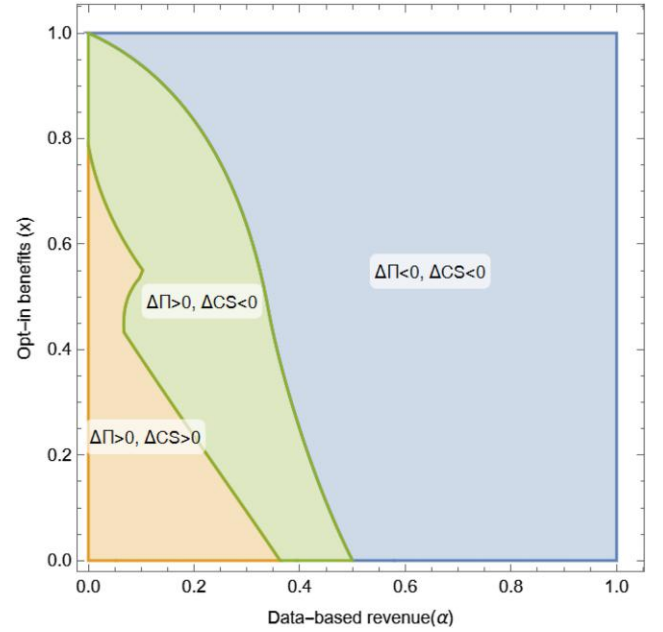


Figure A.2 illustrates Proposition A.4. As before, the two dashed lines are drawn to indicate Regions I–III. The blue-shaded region labeled $\Delta CS > 0$ is where the equilibrium consumer surplus is larger after the GDPR, and the yellow-shaded region labeled $\Delta CS < 0$ is where it is smaller after the GDPR. The line dividing these two regions is made up of three pieces: The lowermost part corresponds to the case where $\alpha < \alpha_1(x)$ (Region I) and is defined by $\alpha_7(x)$ stated in Proposition A.4; the curve in the middle corresponds to the case where $\alpha_1(x) \leq \alpha < \alpha_2(x)$ (Region II) and is defined by $\alpha_8(x)$; and the uppermost part corresponds to the case where $\alpha \geq \alpha_2(x)$ (Region III) and is defined by $\alpha_9(x)$. As shown in the figure, for given values of x , the GDPR increases consumer surplus for smaller values of α but decreases it for larger values of α . In addition, the set of (x, α) that leads to larger consumer surplus is smaller than the set of (x, α) that leads to larger profit, as shown in Figures A.1 and A.2. This is because the price increase following the GDPR partially offsets the benefits to consumers.

Figure A.3 combines Figures A.1 and A.2 and shows the changes in total surplus. After the GDPR, total surplus increases in the region where $\Delta\Pi > 0$ and $\Delta CS > 0$ and decreases in the region where $\Delta\Pi < 0$ and $\Delta CS < 0$. In the region where $\Delta\Pi > 0$ and $\Delta CS < 0$, it increases after the GDPR if and only if $|\Delta\Pi| > |\Delta CS|$. Consistent with our main results, the GDPR is more likely to improve welfare for small values of α but decrease it for large values of α .

Endnotes

¹ Following the GDPR, many countries enacted similar privacy laws or amended existing ones in line with the GDPR. Examples include the California Consumer Privacy Act (CCPA) and Brazil's General Data Protection Law (LGPD) both of which came into effect

in 2020, Singapore's Personal Data Protection Act (PDPA) amended in 2019, South Korea's Personal Information Protection Act (PIPA) amended in 2020, and so on.

² Some of the largest noncompliance penalties are 746 million euros Luxembourg's privacy watchdog (CNPD) imposed on Amazon in 2021, 150 million euros on Google levied by France's privacy watchdog (CNIL) in 2022, and, more recently, 390 million euros Ireland's Data Protection Commission imposed on Meta in 2023.

³ See https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_1166.

⁴ See, for example, "America should borrow from Europe's data-privacy law," *The Economist*, April 5, 2018; "One year on, GDPR needs a reality check," *Financial Times*; June 30, 2019, "How GDPR is failing," *Wired*, May 23, 2022.

⁵ As potential beneficial effects of the GDPR, Godinho de Matos and Adjerid (2022) provide experimental evidence that suggests that the GDPR's enhanced opt-in requirements may improve welfare by providing better privacy protection to consumers and allowing firms to better target their marketing communications.

⁶ This literature is reviewed in Section 2.

⁷ For example, we can consider a model where a fraction of tech-savvy, privacy-conscious consumers make optimal opt-in decisions, and the rest always opt in. We can think of the GDPR as increasing the fraction of the first group of consumers.

⁸ Another interpretation is that the GDPR allowed firms to credibly exercise second-degree price discrimination by offering a menu of {(price for the service, no opt-in benefits), (price for the service, positive opt-in benefits)}. For example, many German news websites offer free access to its content subject to advertising and tracking or a paid subscription without advertising and tracking. Some examples are <https://abo.spiegel.de/de/c/microsites/werbefreileisen/abo> and <https://www.faz.net/faz-net-services/>.

⁹ Gopal et al. (2023) also derive a similar conclusion although welfare-reducing effect of privacy management stems from increased third-party data sharing.

¹⁰ Cong and Matsushima (2023) also consider data management by consumers in a two-dimensional Hotelling model where data collected in one market can be used in another market.

¹¹ Another related issue is data ownership given the public good nature of data (Jones and Tonetti 2020, Dosis and Sand-Zantman 2023). For a review of the literature on privacy, see Acquisti et al. (2016) and Acquisti (2023).

¹² In addition, based on opt-in consumers' data, sellers can infer preference of opt-out consumers, which can lead to higher prices and create negative pecuniary externalities (Belleflamme and Vergote 2016, Braghieri 2017).

¹³ In the baseline model, we assume the consumer expects her actual privacy cost to be equal to the maximum possible privacy cost. In Section 6.2, we consider the case where the expected privacy cost is a fraction of the maximum possible privacy cost with the fraction depending on the firm's revenue model.

¹⁴ In Section 6.1, we discuss the case where v and c are correlated.

¹⁵ By opt-in purchase, we mean more than sharing data with the firm; it also allows the firm to share or sell data to third parties. Likewise, opt-out purchase prevents the firm from selling or sharing personal information with third parties, as stipulated in the CCPA Section 120.

¹⁶ Given that the highest possible privacy cost is one, we consider the nontrivial case where $x < 1$.

¹⁷ As an extension of the baseline model, we considered the case where x is chosen endogenously so that the firm offers two versions of its service, p for opt-out consumers, and (p, x) for opt-in

consumers. This does not change our qualitative results relevant to the GDPR's welfare effects. Our results are also robust when there is a constant marginal cost of providing opt-in benefits. The details are available upon request.

¹⁸ Gans (2022) presents a model where a zero price can be an optimal choice by a monopolistic firm under the assumption of free disposal and the presence of a mass of nongeneric consumers. In our model, a zero price, or even a negative price, can be an optimal choice for businesses if they earn significant data-based revenue. In both cases, price is the relevant strategic variable whether it is zero or even negative.

¹⁹ As we discuss in Section 6.6, many online businesses with a data-based revenue model respond to privacy regulations by exploring new revenue sources such as paid subscriptions or tiered services with differential pricing. This indicates a prominent role price plays in these businesses.

²⁰ See <https://www.reuters.com/article/us-france-google-fine-idUSBREA0719U20140108/>.

²¹ The GDPR's Art. 83(5) specifies that the fine for infringement can be up to 20 million euros or 4% of global turnover of the preceding financial year, whichever is higher. For example, the Luxembourg National Commission for Data Protection imposed 746 million euros on Amazon in 2021 for tracking user data without acquiring appropriate consent or providing the means to opt out from tracking (<https://www.politico.eu/article/amazon-fined-e746m-for-violating-privacy-rules/>).

²² Note that the restriction $x - 1 \leq p$ allows the possibility that the firm may choose a negative price because $x < 1$ by assumption. This may happen when the firm's revenue is largely data based, that is, large α , in which case the firm may subsidize consumers' purchase of its service with a view to monetizing their data.

²³ We use $\hat{\cdot}$ to indicate the regime before the GDPR and $\tilde{\cdot}$ for the regime after the GDPR.

²⁴ The first-order condition is also sufficient. That is, we can show that the solution to the first-order condition $\hat{p}^*$ is the unique extreme value that maximizes $\hat{\Pi}$ within the relevant range corresponding to case 1a and case 1b. The details are provided in the Online Appendix.

²⁵ As shown in the appendix, both case 1a and 1b equilibria are possible before the GDPR when $x \leq 1/2$, and both case 2a and 2b equilibria are possible after the GDPR when $x \leq 2 - \sqrt{2} \approx 0.585$.

²⁶ For example, Nielsen Mobile App pays users redeemable reward points for using its app and, in return, collects data by tracking users' phone usage.

²⁷ We have $0 < v(p) < 1$ if and only if $x < p < 1 + x$. But it is easy to see that profit decreases in p when $p > 1$, hence case 2a becomes $x < p \leq 1$.

²⁸ Unlike the case before the GDPR, the firm will always choose a nonnegative price after the GDPR. It is because consumers with $v \geq p$ and $c > x$ choose opt-out purchase, implying that $p = 0$ leads to the market to be fully covered: consumers with $c > x$ choose opt-out purchase and the rest of consumers choose opt-in purchase. Thus, choosing a negative price cannot increase demand further.

²⁹ Godinho de Matos and Adjerid (2022) report experimental evidence that suggests an alternative channel that the GDPR can generate benefits to advertisers. That is, the GDPR can lead to varying amounts of data collected from different types of data, which can help improve targeting capabilities by advertisers.

³⁰ The remaining case is for intermediate values of α where the comparison is between case 1b equilibrium before the GDPR and case 2a equilibrium after the GDPR. We omit the discussions for brevity, as our main focus is on the two polar cases explained above.

³¹ A study by Pew Research Center (2019) suggests that individuals who are less concerned about privacy are more likely to share more personal information on social media.

³² We thank an anonymous reviewer for suggesting this extension.

³³ For example, the business model of financial institutions is predominantly service based, although some banks may monetize customer data by selling them to third parties. Nevertheless, there are multiple incidents of high-profile data breaches at banks, exposing customers to significant privacy risks. See, for example, “The biggest data leaks and how to prevent them from repeating,” *Forbes*, October 23, 2023, <https://www.forbes.com/councils/forbesbusinesscouncil/2023/10/23/the-biggest-data-leaks-and-how-to-prevent-them-from-repeating/>.

³⁴ Focusing on the case $\alpha \in [0, 1]$ is at no loss of our main insight. In all the figures that accompany our general results provided in the appendix, we consider the case where $\alpha \leq 1$. In addition, in all the results presented in Tables 4–6, the critical threshold values of α are less than one. We do not expect our main insight to change for other functional forms for f insofar as f is an increasing function of α bounded above by one.

³⁵ Management accounting can also play a crucial role by developing performance measures based on which to provide incentives to each revenue center in a way that can mitigate such conflicts.

³⁶ See a blog post by Larry Page, Google’s co-founder, <https://blog.google/alphabet/google-alphabet/>.

³⁷ Twitter eventually acquired Gnip in 2014 to expand its own data analytics capabilities.

³⁸ See <https://www.bbc.com/news/technology-67226394>.

³⁹ See <https://help.twitter.com/en/using-x/x-premium>.

⁴⁰ Our preliminary work in this direction shows nuanced effects of versioning on market outcomes, depending on the underlying market structure. When versioning can be offered credibly, the monopolistic firm is always better off but competing firms are generally worse off.

⁴¹ The Online Appendix provides the full details of solving the firm’s problem.

⁴² The Online Appendix provides the full details of solving the firm’s problem.

References

- Acemoglu D, Makhdoumi A, Malekian A, Ozdaglar A (2022) Too much data: Prices and inefficiencies in data markets. *Amer. Econom. J. Microeconom.* 14(4):218–256.
- Acquisti A (2023) The economics of privacy at a crossroads. Goldfarb A, Tucker C, eds. *The Economics of Privacy* (University of Chicago Press, Chicago), 21–71.
- Acquisti A, Brandimarte L, Loewenstein G (2015) Privacy and human behavior in the age of information. *Science* 347(6221):509–514.
- Acquisti A, Taylor C, Wagman L (2016) The economics of privacy. *J. Econom. Literature* 54(2):442–492.
- Amaldoss W, Du J, Shin W (2024) Pricing strategy of competing media platforms. *Marketing Sci.* 43(3):469–496.
- Anderson SP, Gans JS (2011) Platform siphoning: Ad-avoidance and media content. *Amer. Econom. J. Microeconom.* 3(4):1–34.
- Aridor G, Che Y-K, Salz T (2023) The effect of privacy regulation on the data industry: Empirical evidence from GDPR. *RAND J. Econom.* 54(4):695–730.
- Batikas M, Liu Y, Ozalp H, Miric M (2023) Impact of privacy regulation on experimentation and innovation. *Acad. Management Proc.* 2023(1):17060.
- Belleflamme P, Vergote W (2016) Monopoly price discrimination and privacy: The hidden cost of hiding. *Econom. Lett.* 149:141–144.
- Bergemann D, Bonatti A (2015) Selling cookies. *Amer. Econom. J. Microeconom.* 7(3):259–294.
- Bergemann D, Bonatti A, Gan T (2022) The economics of social data. *RAND J. Econom.* 53(2):263–296.
- Bessen J, Impink SM, Reichensperger L, Seamans R (2020) GDPR and the importance of data to AI startups. Preprint, submitted April 15, <https://dx.doi.org/10.2139/ssrn.3576714>.
- Braghieri L (2017) Targeted advertising and price discrimination in intermediated online markets. Preprint, submitted November 20, <https://dx.doi.org/10.2139/ssrn.3072692>.
- Campbell J, Goldfarb A, Tucker C (2015) Privacy regulation and market structure. *J. Econom. Management Strategy* 24(1):47–73.
- Chaudhury RD, Choe C (2023) Digital privacy: GDPR and its lessons for Australia. *Australian Econom. Rev.* 56(2):204–220.
- Chen Z (2022) Privacy costs and consumer data acquisition: An economic analysis of data privacy regulation. Preprint, submitted April 27, <https://dx.doi.org/10.2139/ssrn.4085923>.
- Chen Z, Choe C, Matsushima N (2020) Competitive personalized pricing. *Management Sci.* 66(9):4003–4023.
- Cheyre C, Leyden BT, Baviskar S, Acquisti A (2023) The impact of Apple’s App Tracking Transparency framework on the app ecosystem. Preprint, submitted May 25, <https://dx.doi.org/10.2139/ssrn.4453463>.
- Choe C, King S, Matsushima N (2018) Pricing with cookies: Behavior-based price discrimination and spatial competition. *Management Sci.* 64(12):5669–5687.
- Choi JP, Jeon D-S, Kim B-C (2019) Privacy and personal data collection with information externalities. *J. Public Econom.* 173:113–124.
- Cong J, Matsushima N (2023) The effects of personal data management on competition and welfare. Working paper, ISER Discussion Paper No. 1201, Institute of Social and Economic Research, Osaka University, Osaka, Japan.
- Congiu R, Sabatino L, Sapi G (2022) The impact of privacy regulation on web traffic: Evidence from the GDPR. *Inform. Econom. Policy* 61:101003.
- Dosis A, Sand-Zantman W (2023) The ownership of data. *J. Law Econom. Organ.* 39(3):615–641.
- Fainmesser IP, Galeotti A, Momot R (2023) Digital privacy. *Management Sci.* 69(6):3157–3173.
- Gans JS (2022) The specialness of zero. *J. Law Econom.* 65(1):157–176.
- Ghose A (2017) *Tap: Unlocking the Mobile Economy* (MIT Press, Cambridge, MA).
- Godinho de Matos M, Adjerid I (2022) Consumer consent and firm targeting after GDPR: The case of a large telecom provider. *Management Sci.* 68(5):3330–3378.
- Goldberg SG, Johnson GA, Shriver SK (2024) Regulating privacy online: An economic evaluation of the GDPR. *Amer. Econom. J. Econom. Policy* 16(1):325–358.
- Goldfarb A, Tucker C (2012) Shifts in privacy concerns. *Amer. Econom. Rev.* 102(3):349–353.
- Gopal RD, Hidaji H, Kutlu SN, Patterson RA, Yaraghi N (2023) Law, economics, and privacy: Implications of government policies on website and third-party information sharing. *Inform. Systems Res.* 34(4):1375–1397.
- Hagiu A, Wright J (2023) Data-enabled learning, network effects and competitive advantage. *RAND J. Econom.* 54(4):638–667.
- Ichihashi S (2021) The economics of data externalities. *J. Econom. Theory* 196:105316.
- Ichihashi S (2023) Dynamic privacy choices. *Amer. Econom. J. Microeconom.* 15(2):1–40.
- Janßen R, Kesler R, Kummer ME, Waldfogel J (2022) GDPR and the lost generation of innovative apps. NBER Working Paper No. 30028, National Bureau of Economic Research, Cambridge, MA.
- Jentzsch N, Sapi G, Suleymanova I (2013) Targeted pricing and customer data sharing among rivals. *Internat. J. Industrial Organ.* 31:131–144.

- Jia J, Jin GZ, Wagman L (2021) The short-run effects of the General Data Protection Regulation on technology venture investment. *Marketing Sci.* 40(4):661–684.
- Johnson EJ, Bellman S, Lohse GL (2002) Defaults, framing and privacy: Why opting in-opting out. *Marketing Lett.* 13(1):5–15.
- Johnson GA, Shriver SK, Du S (2020) Consumer privacy choice in online advertising: Who opts out and at what cost to industry? *Marketing Sci.* 39(1):33–51.
- Johnson GA, Shriver SK, Goldberg SG (2023) Privacy and market concentration: Intended and unintended consequences of the GDPR. *Management Sci.* 69(10):5695–5721.
- Jones CI, Tonetti C (2020) Nonrivalry and the economics of data. *Amer. Econom. Rev.* 110(9):2819–2858.
- Ke TT, Sudhir K (2023) Privacy rights and data security: GDPR and personal data markets. *Management Sci.* 69(8):4389–4412.
- Lin S (2020) Two-sided price discrimination by media platforms. *Marketing Sci.* 39(2):317–338.
- Lin T (2022) Valuing intrinsic and instrumental preferences for privacy. *Marketing Sci.* 41(4):235–253.
- Macha M, Foutz NZ, Li B, Ghose A (2024) Personalized privacy preservation in consumer mobile trajectories. *Inform. Systems Res.* 35(1):249–271.
- Machuletz D, Böhme R (2020) Multiple purposes, multiple problems: A user study of consent dialogs after GDPR. *Proc. Privacy Enhancing Tech.* 2020(2):481–498.
- Matte C, Bievola N, Santos C (2020) Do cookie banners respect my choice?: Measuring legal compliance of banners from IAB Europe's transparency and consent framework. *Proc. IEEE Sympos. Security Privacy* (IEEE, New York), 791–809.
- Miklós-Thal J, Goldfarb A, Haviv AM, Tucker C (2024) Digital hermits. *Marketing Sci.* 43(3):697–708.
- Nouwens M, Llicardi I, Veale M, Karger D, Kagal L (2020) Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence. *Proc. CHI Conf. Human Factors Comput. Systems* (Association for Computing Machinery, New York), 1–13.
- Obar JA, Oeldorf-Hirsch A (2020) The biggest lie on the Internet: Ignoring the privacy policies and terms of service policies of social networking services. *Inform. Comm. Soc.* 23(1):128–147.
- Peukert C, Bechtold S, Batikas M, Kretschmer T (2022) Regulatory spillovers and data governance: Evidence from the GDPR. *Marketing Sci.* 41(4):318–340.
- Pew Research Center (2019) Americans and privacy: Concerned, confused and feeling lack of control over their personal information. (November 15), <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/>.
- Schmitt J, Miller KM, Skiera B (2021) The impact of privacy laws on online user behavior. Preprint, submitted March 16, <https://dx.doi.org/10.2139/ssrn.3774110>.
- Utz C, Degeling M, Fahl S, Schaub F, Holz T (2019) (Un)informed consent: Studying GDPR consent notices in the field. *Proc. ACM SIGSAC Conf. Comput. Comm. Security* (Association for Computing Machinery, New York), 973–990.