Dec 12th, 12:00 AM

Privacy Versioning for Competitive Advantage

José Parra-Moyano
Copenhagen Business School, jpm.digi@cbs.dk

Sameer Mehta
Erasmus University Rotterdam, sameer@illinois.edu

Privacy Versioning: Accommodating the Demands of the Next Generation

Short Paper

José Parra-Moyano
Copenhagen Business School
Howitzvej 60, 2000 Frederiksberg,
Copenhagen, Denmark
jpm.digi@cbs.dk

Sameer Mehta
Rotterdam School of Management
Burgemeester Oudlaan 50, 3062 PA
Rotterdam, The Netherlands
mehta@rsm.nl

Abstract

There is increasing tension between the service quality improvements consumers receive when they allow their data to be analyzed by a firm, and the costs they incur in terms of privacy sacrifices. This is motivating firms to explore new models to attract and retain a new generation of privacy-active customers (i.e., customers who act in order to protect their privacy). This paper sets the foundation to solve the mechanism design problem for a firm that offers a continuous set of menus allowing its customers to chose their optimal combination of privacy and price. The solution of the problem shows that the relationship between prices and the amount of data shared is non-monotonic. This is a surprising result that may contribute to a better understanding of the privacy paradox, as well as to help scholars and practitioners to push the known boundaries of privacy-based versioning.

Keywords: Mechanism Design, Privacy Paradox, Privacy Versioning, Subscription Model

Introduction

In the era of personal data digitalization (Leidner and Tona 2021), there is an inherent tension between analyzing customers' data to increase the quality of the offered products and services, and respecting the privacy of those customers' whose data is analyzed. This tension lies at the very core of the discussion that—scholars and practitioners alike—are currently having about privacy and analytics (Schneider et al. 2017).

Recent research suggests that while consumers have thus far felt very comfortable letting firms analyze their data (Spiekermann et al. 2001), the new generation of consumers is becoming "privacy active", meaning that they are starting to act in order to protect their privacy (Redman and Waitman 2020). This new evidence is at odds with the established notion of the *Privacy Paradox* (the phenomenon whereby people say that they value privacy highly, yet in their behavior relinquish their personal data for very little in exchange). Contrary to the depiction of online sharing behaviors as careless, consumers do fundamentally care about online privacy (Acquisti et al. 2020), and they are sometimes even willing to pay a price premium to purchase goods from more privacy-protective merchants (Tsai et al. 2011).

As this tension between privacy protection and data analytics grows, and acknowledging the business benefits of addressing customers' privacy needs (Gimpel et al. 2018), firms are confronted with the following question: *What is the optimal amount of data we should analyze in order to offer our consumers the best balance between quality and privacy?* While some firms have decided to not analyze any customers' data at all and have therefore given up on the potential benefits of customers profiling (Mikalef et al. 2019), others

are starting to consider a sort of *privacy versioning* for digital products and services, whereby customers can freely chose different levels of privacy and therefore quality. For firms generating their revenue from selling targeted advertisement (such Google or the Meta Platform, formerly Facebook) the trade-off is only between privacy and quality. However, firms generating their revenue from subscription fees, can add another variable to this problem: the price (Kummer and Schulte 2019; Soleymanian et al. 2019). Given that in this context there is a trade-off between privacy and quality, firms generating their revenue from subscription fees can offer a set of menus that let consumers choose their optimal combination of privacy, quality, and price. By implementing such a privacy-based screening mechanism, firms can attract and retain customers that are very different to one another when it comes to their appetite for privacy (i.e., heterogeneous in their sensitivity to privacy). This idea, expressed in simple words, implies that every customer can decide, basing on his or her privacy preferences, which version of the digital product or service he or she is going to receive. For the resulting service and privacy level, every customer gets a personalized price. This mechanism enables the firm to develop several versions of their products and services in order for the firm to attract more consumers, namely the consumers that in the absence of these versions would not find the single version of the product or service appealing enough to pay for it.

Since this practice is still in its infancy, we consider important to pose the following question: *What is the optimal relationship between privacy, quality, and price that subscription-model firms should offer in order to attract the broadest possible set of customers?* Basing on the mechanism design literature (Chellappa and Shivendu 2010; Casadesus-Masanell and Hervas-Drane 2015; Gal-Or et al. 2018), we propose a mechanism—with a unique equilibrium—that enables firms to offer an optimal, privacy-based price to each individual customer. Surprisingly, this mechanism reveals that, under some circumstances, greater data disclosure (i.e., less privacy) is not always associated with a lower price.

This paper aims to offer interesting insights that can be further developed by scholars to better understand the trade-offs between privacy, quality, and price, in order to offer new mechanisms for firms to satisfy the heterogeneous privacy appetites of consumers. At an applied level, the results shown in this paper may have direct implications for firms offering subscription models for information goods, as well as for firms trying to cope with consumers' increasing appetite for privacy.

The remainder of this paper is structured as follows. In the next section we describe the background of the problem and provide a short literature review. We continue by defining and solving a mechanism enabling privacy-based screening, whose results we later discuss. We finish by describing the limitations of our analysis and proposing new questions to be asked in the context of this problem to continue exploring this area.

Literature Review

This section briefly introduces the most relevant literature on privacy, quality, and competitive advantages, and revises the relevant literature in the field of mechanism design.

Literature on privacy, quality, and competitive advantages

There exists a trade-off between the use of personal data to improve the quality of the offered products and services, and the implementation of measures to protect data privacy (Schneider et al. 2017). Firms offering information goods (goods that can be digitized) are some of the key actors affected by this trade-off, since they are particularly well positioned to monetize data by embedding analytics into their products and services in order to increase the perceived quality of these products and services (Davenport 2013).

Some examples of firms embedding "data driven innovations" (Dinter and Kräemer 2018) within their services and using data as a factor of production (Parra-Moyano et al. 2020) are the video streaming platforms, Netflix, Amazon Prime Video, and HBO, which incorporate insights gained by analyzing their clients' behavior to make personalized content recommendations. Another example of this type of firms are the ones offering sports tracking applications and/or weareables, like Runtastic, Fitbit, or Adidas Runners, which analyze customers' data to provide them with personalized advice, encouraging their healthy habits. Yet another example of this type of firms are insurance companies, such as American Family Insurance, Mapfre,

and more recently Tesla (Holland and Kavuri 2022), that are offering usage-based insurance (UBI) driving policies (Seger and Figl 2019) that enable them to provide its customers with feedback on driving performance and individually targeted price discounts based on customer's driving behaviors (Soleymanian et al. 2019). By letting service providers analyze their data, consumers benefit from better services. In doing so, however, they also sacrifice part of their privacy. Streaming platforms learn about their customers' habits and preferences; sports tracking applications glean health-related information on their customers; insurance companies offering UBI policies learn about their customers' mobility and driving habits. These examples reveal the existing trade-off between quality and privacy.

In this context, increasingly more research is considering data privacy measures as an opportunity to create a competitive advantage. In this vein, it has been shown that firms aiming to improve customer satisfaction by superior privacy protection should elicit the demands of their specific target customers (Gimpel et al. 2018). Moreover, it has been proven that appropriate management of data privacy issues may have positive implications on customer satisfaction (Preibusch 2013), and that data privacy strategies which exceed the level of data privacy required by laws and regulations are deemed superior to the ones that simply comply with laws and regulations (Sarathy and Robertson 2003).

One example of a firm implementing privacy preserving initiatives to create a competitive advantage is Apple, which has recently launched privacy labels for applications in its App Store. These labels aim to give customers of the App Store an easier way to understand what sort of information each application collects about them, and with which purpose this information is used. Additionally, Apple has also launched an iOS upgrade (Apple 2022) that provides users with significantly more control over how, and by whom, they are tracked across platforms (by denying passage of the unique identifier). Similarly, Google has launched "privacy suggestions", which invite the users of Google services to define for how long their data is stored on Google's premises. This initiative gives users more control over their data and enables them to adapt products and services to their respective privacy preferences: those users who are comfortable with sharing their data and with getting a more personalized service in return can continue doing so, while those who care more about privacy can reduce the amount of data they share, and still benefit from using Google services.

We consider that these positions regarding privacy preservation and quality (the one defending a trade-off between quality and privacy, and the that considers data privacy measures as an opportunity to create a competitive advantage) are two sides of the same coin. Specifically, we consider that the trade-off between quality and privacy exists, but that at the same time it can be exploited by firms to create a competitive advantage. This can be achieved by what we call *privacy versioning*, a term we have coined to refer to those initiatives that enable customers to freely chose the level of privacy (and therefore quality) they get when using a firm's products or services. Firms generating their revenue from subscription fees, can (or need) to add an additional dimension to this privacy-quality bundle, namely the price. Finding a mechanism to determine the optimal relationship between privacy, quality, and price, would enable firms to screen their customers' preferences and to attract and retain customers that are very different to one another when it comes to their appetite for privacy. Such a mechanism would enforce a privacy-based pricing.

Literature on privacy-based pricing

Mechanism design is a subfield of game theory that aims to designing institutions that determine decisions as a function of the information that is known by the individuals in the economy in order to achieve a desired outcome (Myerson 1983). Recent work has blurred the border between mechanism design and computer science (Papadimitriou 2001), showcasing how mathematical analysis is likely to prove useful tools for understanding problems in the field of Information Systems (IS). Given the nature of our research question, we study the mechanism design literature to learn the current state of affairs in problems related to individual privacy choices.

The idea of enabling customers to chose their desired privacy preferences is not new, and has already been proposed. One example of this type of analysis is the one conducted by (Chellappa and Shivendu 2010), that examines pricing strategies for online vendors in a market where consumers have heterogeneous concerns about privacy. Another example of this type of work is the one conducted by (Casadesus-Masanell and Hervas-Drane 2015), which considers a market where firms set prices and disclosure levels for consumer

information, and consumers observe both before deciding which firm to patronize and how much information to provide. This work shows that higher competition intensity between the service providers does not improve consumer privacy when consumers exhibit low willingness to pay. In a similar vein, the work conducted by (Gal-Or et al. 2018) studies the effect of user privacy concerns on competition between online advertising platforms, showing that the presence of heterogeneity in the user and the advertiser populations with respect to their preferences for targeting leads to differentiation between platforms.

All these papers analyze online providers generating their revenue from selling targeted advertisement (i.e., providers that don't charge a monetary price to the users who sacrifice their privacy and that perceive the quality of the product or service). However, these papers do not consider firms generating their revenue from the subscription fees of the consumers (like video streaming platforms, sports tracking applications, and insurance companies offering usage-based insurance driving policies), and not from selling targeted advertisement. There is therefore a research gap in this type of analysis. We consider that studying privacy versioning for firms generating revenues streams from the subscription fees of the consumers is interesting, since they can offer different prices to their consumers, something that firms deriving their revenues from selling targeted advertisement cannot do. For this reason, in the next section we build on the mechanism design literature to derive a model that helps us to answer our research question: *What is the optimal relationship between privacy, quality, and price that subscription-model firms should offer in order to attract the broadest possible set of customers?*

A Model for Privacy-Based Screening

We consider a firm that sells an information good to a unit mass of customers. In the process of using the good, the customers share their personal data with the firm. On the one hand, the firm uses this data to improve the quality of the good, which in turn benefits all the customers in general, but particularly the quality perceived by the customer whose data is analyzed. On the other, the customers incur a privacy-based disutility when sharing their data with the firm. Customers are heterogeneous in this disutility, and are indexed by their type, θ, which determines the extent of the disutility they incur when sharing their data. The firm knows its customers' type distribution but does not observe each specific customer's type.

Let $F(\theta)$ denote the probability distribution of the types in the customer population on the support $[\theta_{\mathrm{l}}, \theta_{\mathrm{h}}]$ and let $f(\theta)$ denote the corresponding density function. For simplicity,[1] this paper assumes that $\theta \sim U(0,1)$.

We define our model building on the idea that consumers are heterogeneous in their appetite for privacy (Casadesus-Masanell and Hervas-Drane 2015; Chellappa and Shivendu 2010; Gal-Or et al. 2018). Moreover, we consider that the very consumers that have a higher valuation of the good are also those that incur a higher disutility from sharing their data, which is similar to the considerations made by (Casadesus-Masanell and Hervas-Drane 2015) and (Chellappa and Shivendu 2010)).

Consumers' Preferences:

Let V denote the base utility that a customer obtains from consuming the information good without sharing any data with the firm. The preferences of a customer of type θ are represented by the following utility function:

$$U(\theta, q, p) = V + \beta V q - \theta c q^2 - p, \tag{1}$$

where q is the quality of the data shared and p is the price paid by the customer. Note that, in line with (Casadesus-Masanell and Hervas-Drane 2015), in this paper the amount of data and the quality of data are treated as equivalent. The constant $\beta \geq 0$ determines the extent of the additional utility that customers obtain over the base utility when they share their data, and the constant $c \geq 0$ determines the extent of disutility that customers incur when sharing their data. This paper assumes that $q \in [0,1]$.

The base utility V that customers obtain by consuming a good consists of two components. The first is the

[1] Note that this analysis is valid for all distributions that are *regular*. A distribution is said to be *regular* if the function $\psi(\theta) := \theta + \frac{F(\theta)}{f(\theta)}$ is non-decreasing in θ.

intrinsic base utility of the good if no customer shares her data with the firm. The intrinsic utility is denoted by $\alpha \in [0,1]$. The second component results from the improvements that the firm makes to the good as a consequence of data aggregation from participating customers. Naturally, this base utility is proportional to the aggregate quality of the data shared by the participating customers under mechanism μ. If a customer of type θ shares data of quality $q(\theta)$ with the firm, then it is assumed that the aggregate quality of data is $\int_{\theta_\mathrm{l}}^{\theta_\mathrm{h}} q(\theta) f(\theta) d\theta$. Without loss of generality, the maximum value of the base utility is normalized to 1. Then, the base utility of the good is

$$V = \underbrace{\alpha}_{\text{intrinsic base utility}} + \underbrace{(1-\alpha) \int_{\theta_\mathrm{l}}^{\theta_\mathrm{h}} q(\theta) f(\theta) d\theta}_{\text{base utility from data aggregation}} . \tag{2}$$

The Firm's Mechanism Design Problem

Using the Revelation Principle Myerson 1981, this paper restricts its attention, without loss of generality, to the class of direct mechanisms that are incentive compatible and individually rational for consumers. In this context, a direct mechanism μ is characterized by a pair of functions (q_μ, p_μ), where $q_\mu : [\theta_\mathrm{l}, \theta_\mathrm{h}] \to [0,1]$ is a data-quality allocation function and $p_\mu : [\theta_\mathrm{l}, \theta_\mathrm{h}] \to \mathbb{R}$ is a payment function.

Let V_μ denote the base utility under a mechanism μ. Note that this base utility is determined using the aggregate quality of the data shared by customers under the mechanism μ. However, the quality of the data shared by customers under the mechanism μ itself depends on V_μ. Following the standard assumptions of rational expectations it results that upon observing the mechanism μ, the customers form a belief regarding the base utility V_μ and make their decision to reveal their type θ. These decisions in turn result in a base utility, V_μ, that is consistent with the belief of the customers.

Let $U_\mu(\hat{\theta}; \theta, t)$ denote the utility to a customer of type θ who reveals her type as $\hat{\theta}$ under mechanism μ. Then,

$$U_\mu(\hat{\theta}; \theta) = V_\mu + \beta V_\mu q_\mu(\hat{\theta}) - c\theta q_\mu(\hat{\theta})^2 - p_\mu(\hat{\theta}). \tag{3}$$

The incentive-compatibility (ic) and the individual-rationality (ir) constraints can be stated as follows:

$$U_\mu(\theta;\theta) \geq U_\mu(\hat{\theta};\theta)\ \forall \theta \in [\theta_\mathrm{l}, \theta_\mathrm{h}]\,; \tag{ic}$$
$$U_\mu(\theta;\theta) \geq 0\ \forall \theta \in [\theta_\mathrm{l}, \theta_\mathrm{h}]\,. \tag{ir}$$

The mechanism design problem for the firm can be stated as follows:

$$\max_{\mu}\ \mathbb{E}_\theta\left[p_\mu(\theta)\right]\ \text{s.t. (ic), (ir).} \tag{P}$$

The following results, whose proof we don't include in this paper due to the space limitation, but that can be shard upon request, state the equilibrium base utility and an optimal solution to problem P.

Theorem 1 *If* $\frac{c}{\beta} \leq \frac{1}{4}$*, then the equilibrium base utility is*

$$V_\text{opt} = 1, \tag{4}$$

and the opt *mechanism defined by*

$$q_\text{opt}(\theta) = 1\ \forall \theta \in [0,1], \tag{5}$$
$$p_\text{opt}(\theta) = 1 + \beta - c\ \forall \theta \in [0,1] \tag{6}$$

is an optimal solution to problem P.

If $\frac{c}{\beta} \geq \frac{1}{4}$*, the equilibrium base utility is the unique solution to the following equation:*

$$\alpha + \frac{(1-\alpha)\beta V_{\text{opt}}}{4c}\left(1 - \log\left(\frac{\beta V_{\text{opt}}}{4c}\right)\right) - V_{\text{opt}} = 0, \tag{7}$$

and the opt *mechanism defined by*

$$q_{\text{opt}}(\theta) = \begin{cases} 1 & \text{if } 0 \leq \theta \leq \frac{\beta V_{\text{opt}}}{4c} \\ \frac{\beta V_{\text{opt}}}{4c\theta} & \text{if } \frac{\beta V_{\text{opt}}}{4c} \leq \theta \leq 1, \end{cases} \tag{8}$$

$$p_{\text{opt}}(\theta) = V_{\text{opt}}\left(1 + \beta q_{\text{opt}}(\theta)\right) - c\theta q_{\text{opt}}(\theta)^2 - \int_{\theta}^{1} c q_{\text{opt}}(x)^2 dx \tag{9}$$

is an optimal solution to problem P.

Illustration of the result

Figure 1 depicts the relationship between the quality (or amount) of the data shared by the customer and the price that the firm should charge for the good when implementing the optimal mechanism. At this stage it is important to note that a higher degree of privacy disclosure implies a lower level of privacy. This figure illustrates how the optimal price is non-monotonic in the quality of shared data, and how customers sharing data of a relatively high quality are charged more than certain customers who share data of a lesser quality. This result, which might seem counter-intuitive at first, is explained by the fact that customers experience an increased utility when sharing more data. Hence, for low values of θ, the increased quality of the good perceived by sharing more data compensates for the disutility of the sacrificed privacy.

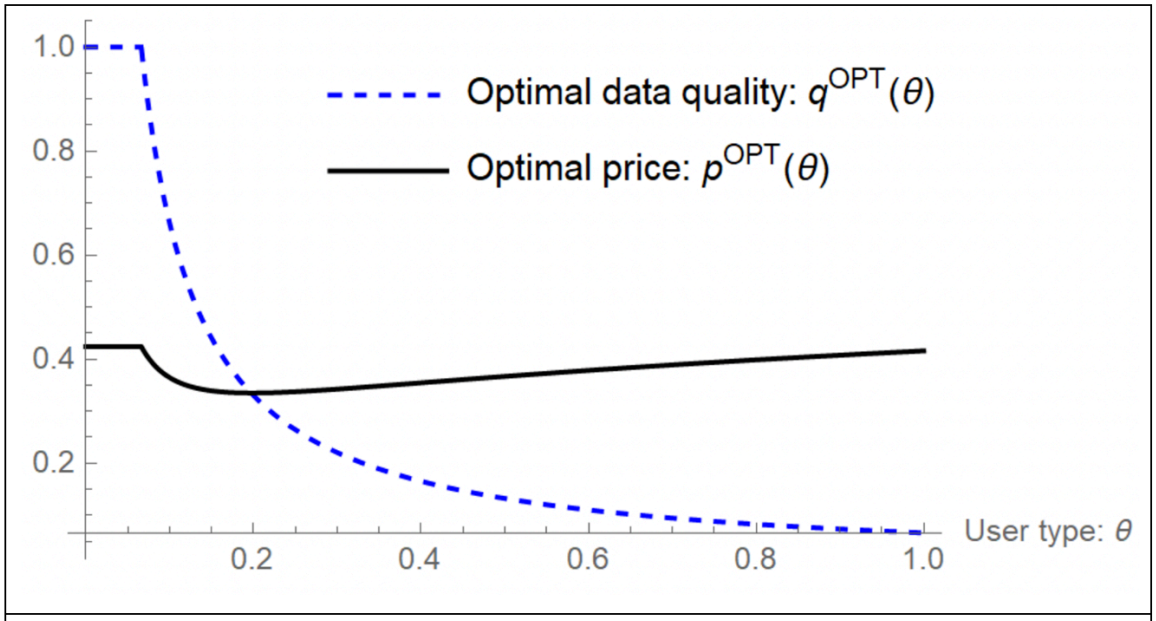

Figure 1. Optimal Data Quality and Optimal Payment Under the OPT Mechanism

Discussion

In this paper we have derived the concept of privacy-based versioning, and defined and solved the mechanism design problem of a firm generating its revenue from the subscription fees paid by its customers and offering a set of privacy and price menus to its customers. By establishing a relationship between the level of

disclosed data (i.e., the privacy level), the perceived quality of the good, and the price paid for an information good, the paper offers an approach to define the optimal set of privacy-price menus a firm needs to offer, in order to optimally satisfy its customers' needs. The mechanism we propose is the analytical answer to our research question.

Theoretical Implications

While previous work has thoroughly analyzed how firms can compete in terms of privacy (Chellappa and Shivendu 2010; Casadesus-Masanell and Hervas-Drane 2015; Gal-Or et al. 2018), to the best of our knowledge non of them has offered an optimal set of menus to let consumers chose their preferred combination of privacy and price. Moreover, non of these papers considers firms generating their revenue from the subscription fees of the consumers (like video streaming platforms, sports tracking applications, and insurance companies offering usage-based insurance driving policies), and not from selling targeted advertisement. Hence, we contribute to the literature by solving a model that enables firms generating their revenues from subscription models to offer a continuous privacy-based versioning to its consumers. The solution to this model enables the firm to offer an optimal price each customer, depending on the level of privacy (and resulting quality) chosen by each customer.

Contrary to what we would be expected, the relationship between the level of privacy chosen by the customer and the price is non-monotonic. Some customers are therefore charged a higher price when they decide to share more data with the firm (i.e., when they chose a lower level of privacy). This is counter-intuitive because we would expect that the more privacy is sacrificed, the lower the required price for the good or service would be.

One explanation for this result might be that by sharing a relatively large amount of their data, customers receive an information good of higher quality. For those customers that experience a low disutility when sacrificing their privacy, the increase in utility due to the good's higher quality is greater than the decrease in utility due to the privacy sacrifice. This insights confirms (in an analytical way) the considerations that data privacy measures are an opportunity to creating a competitive advantage (Sarathy and Robertson 2003; Preibusch 2013; and Gimpel et al. 2018).

Our results might also be interesting, since they can offer a possible explanation of the privacy paradox: While consumers do care about their privacy, the increased utility they perceive by sharing their data compensates for the disutility of sacrificing their privacy. In other words: it is not that consumers do not care about privacy, it is that for many of them, the privacy-related disutility they suffer when giving away their data, is lower than the increase in the quality-related utility they derive when sharing that data. Since the quality increase perceived by the consumers when sharing more data offsets the privacy sacrifice, consumers allow firms to analyze their data, even if they care about their privacy. This insight is in line with the work of (Athey et al. 2017), which explains how consumers are willing to relinquish private data to firms quite freely when incentivized to do so.

Practical Implications

The results presented in this paper imply that firms generating revenue streams from the subscription fees of the consumers and embedding "data driven innovations" (Dinter and Kräemer 2018) within their products and services can benefit from letting customers freely chose their privacy conditions. The price that firms should charge for each privacy level, is the one derived as a solution to the problem presented in Section 3.

Hence, streaming platforms (like Netflix, Amazon Prime Video, and HBO), sports tracking applications and/or weareables (like Runtastic, Fitbit, or Adidas Runners) and insurance companies (like American Family Insurance, Mapfre, and Tesla) can use the results from this paper to continue exploring privacy-based versioning and to derive optimal privacy-price menus to attract new customers and to retain the existing ones. Our results can therefore help firms to compete in privacy to gain a competitive advantage. Note that this competitive advantage stems from the ability to offering different versions of a product or service, which results in a broader set of agents converting into consumers.

Limitations

Naturally, our paper suffers from several limitations. First, our model does not incorporate the notion of versioning directly. Hence, given this model, it is possible to offer a distinct version of the product or service to each consumer. While this is possible in theory, the implementation of such a granular versioning would be highly impractical for the firm. Therefore, future research could incorporate versioning to the model directly, in order to limit the amount of version of the product that are made available to the customers.

Second, we do not consider the cost of data accumulation from the firm's perspective in their current model setup. As data maintenance and processing require substantial infrastructure investment as well as account for a significant portion of operational costs, this aspect of data accumulation could be also incorporated to the model. We posit that incorporating the cost of data accumulation would result in the optimal price for the consumers tolerating more privacy-invasive versions of their goods to increase more than the optimal price for the privacy-active consumers. Should this be the case, then more privacy-preserving version of the product or good would be solved, which establishes an interesting link between the cost of cloud storage and consumers' privacy. Future research is needed in this regard.

Third, the self-disclosing contract is written based on the quantity of shared data. Although data quantity is arguably verifiable (and thereby contractible), its associated costs and benefits are intangible and difficult for customers to assess at the point of contracting. This undermines the eligibility of the proposed menu by the customers.

Fourth, the utility perceived by a customer depends on the data aggregated from all customers, which is difficult for a customer to assess before signing the contract. This difficults the practical implementations of contracts like the one proposed in this paper. Future research could explore how changing contracting on quantity of shared data to contracting on realized service level could help to circumvent this obstacle.

Conclusion

In this paper we have studied the trade-off between the use of personal data to improve the quality of digital products and services, and the implementation of measures to protect data privacy (Schneider et al. 2017). We have shown how, firms offering information goods can benefit from offering a privacy versioning menu to their customers. In light of the fact that the new generation of consumers is becoming more privacy active (Redman and Waitman 2020) and that their concerns with regard to privacy are increasing (Acquisti et al. 2020; Stutzman et al. 2013; Stutzman et al. 2013), the mechanism this paper proposes can help firms to explore new business models: ones in which they version their goods in terms of privacy such that they can attract and retain both the privacy-active consumer and the consumer that will tolerate more privacy-invasive versions of their goods. For this type of contracts to become practical, future research on privacy-based versioning is needed. We expect that the results shown in this paper open new avenues for research on privacy-based versioning and can help scholars and practitioners alike, to push the boundaries of what is considered possible in regard to privacy versioning, and to accommodate the privacy needs of a new consumers' generation.

References

Acquisti, A., Brandimarte, L., and Loewenstein, G. 2020. "Secrets and Likes: The Drive for Privacy and the Difficulty of Achieving It in the Digital Age," *Journal of Consumer Psychology* (30:4), pp. 736–758.

Apple 2022. "About iOS 14 Updates," (available online at https://support.apple.com/en-us/HT211808; accessed Mar. 23, 2022).

Athey, S., Catalini, C., and Tucker, C. 2017. *The Digital Privacy Paradox: Small Money, Small Costs, Small Talk*. NBER Working Papers 23488. National Bureau of Economic Research, Inc, 2017.

Casadesus-Masanell, R. and Hervas-Drane, A. 2015. "Competing with Privacy," *Management Science* (61:1), pp. 229–246.

Chellappa, R. K. and Shivendu, S. 2010. "Mechanism Design for "Free" but "No Free Disposal" Services: The Economics of Personalization Under Privacy Concerns," *Management Science* (56:10), pp. 1766–1780.

Davenport, T. H. 2013. "Analytics 3.0," *Harvard business review* (91:12), pp. 64–72.

Dinter, B. and Kräemer, J. 2018. "Data-driven innovations in electronic markets," *Electron Markets* (28), pp. 403–405.
Gal-Or, E., Gal-Or, R., and Penmetsa, N. 2018. "The Role of User Privacy Concerns in Shaping Competition Among Platforms," *Information Systems Research* (29:3), pp. 698–722.
Gimpel, H., Kleindienst, D., Nüske, N., Rau, D., and Schmied, F. 2018. "The upside of data privacy – delighting customers by implementing data privacy measures," *Electron Markets* (28), pp. 437–452.
Holland, C. P. and Kavuri, A. 2022. "Artificial intelligence and digital transformation of insurance markets," *Journal of Financial transformation* (54:3), pp. 9–210.
Kummer, M. and Schulte, P. 2019. "When Private Information Settles the Bill: Money and Privacy in Google's Market for Smartphone Applications," *Management Science* (65:8), pp. 3470–3494.
Leidner, D. and Tona, O. 2021. "The CARE Theory of Dignity Amid Personal Data Digitalization," *MIS Quarterly* (45) 1, pp. 343–370.
Mikalef, P., Boura, M., Lekakos, G., and Krogstie, J. 2019. "Big data analytics and firm performance: Findings from a mixed-method approach," *Journal of Business Research* (98), pp. 261–276.
Myerson, R. B. 1981. "Optimal Auction Design," *Mathematics of Operations Research* (6:1), pp. 58–73.
Myerson, R. B. 1983. "Mechanism Design by an Informed Principal," *Econometrica* (51:6), pp. 1767–1797.
Papadimitriou, C. 2001. "Algorithms, Games, and the Internet," in *Proceedings of the Thirty-Third Annual ACM Symposium on Theory of Computing,* STOC '01. Hersonissos, Greece: Association for Computing Machinery, pp. 749–753.
Parra-Moyano, J., Schmedders, K., and Pentland, A. S. 2020. "What Managers Need to Know About Data Exchanges," *MIT Sloan Management Review* (61:4), pp. 39–44.
Preibusch, S. 2013. "Guide to measuring privacy concern: Review of survey and observational instruments," *International Journal of Human-Computer Studies* (71:12), pp. 1133–1143.
Redman, T. C. and Waitman, R. M. 2020. "Do You Care About Privacy as Much as Your Customers Do?," *Harvard Business Review* (98:2).
Sarathy, R. and Robertson, C. 2003. "Strategic and Ethical Considerations in Managing Digital Privacy," *Journal of Business Ethics* (46:1), pp. 111–126.
Schneider, M. J., Jagpal, S., Gupta, S., Li, S., and Yu, Y. 2017. "Protecting customer privacy when marketing with second-party data," *International Journal of Research in Marketing* (34:3), pp. 593–603.
Seger, F. and Figl, K. 2019. "Influence Factors for Customer Acceptance of Data-Driven Contracts in Insurance Ecosystems," in *Proceedings of Workshop of Digital Innovation with GIS and Location Analytics, Munich, Germany,* vol. 12, pp. 15–2019.
Soleymanian, M., Weinberg, C. B., and Zhu, T. 2019. "Sensor Data and Behavioral Tracking: Does Usage-Based Auto Insurance Benefit Drivers?," *Marketing Science* (38:1), pp. 21–43.
Spiekermann, S., Grossklags, J., and Berendt, B. 2001. "E-Privacy in 2nd Generation E-Commerce: Privacy Preferences versus Actual Behavior," in *Proceedings of the 3rd ACM Conference on Electronic Commerce,* EC '01. Association for Computing Machinery. Tampa, Florida, USA: Association for Computing Machinery, pp. 38–47.
Stutzman, F., Gross, R., and Acquisti, A. 2013. "Silent Listeners: The Evolution of Privacy and Disclosure on Facebook," *Journal of Privacy and Confidentiality* (4) 2013, p. 2.
Tsai, J. Y., Egelman, S., Cranor, L., and Acquisti, A. 2011. "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study," *Information Systems Research* (22:2), pp. 254–268.