# Privacy Concerns on Social Media Monopoly

Bipasa Datta * Shuyi Lou†

February 27, 2025

**Abstract**

In this paper, we examine privacy issues related to the disclosure of personal information by Internet users on a monopoly social media platform. A user can choose to disclose different types of information about his personal characteristics and can choose how much information from each category to disclose, according to certain trade-offs. By collecting user's disclosed information, the monopoly platform can choose to trade certain proportions of each type of information to a third-party advertiser. It does so by setting different prices for each category of information in order to maximise its profits ensuring participation from the advertiser. We find that, in equilibrium, the user behaves more cautiously with respect to disclosing information about his personal identity whereby he can choose not to reveal any excess information if the risks of being exposed to cyber attacks outweigh the benefits of positive network effects. On the other hand, the user always discloses some information about his other personal characteristics such as his shopping preferences. In equilibrium, when the

*Department of Economics and Related Studies, University of York, York, United Kingdom. Email: bipasa.datta@york.ac.uk. Corresponding author.

†Department of Economics and Related Studies, University of York, York, United Kingdom. E-mail: sl1933@york.ac.uk.

platform collects a positive amount of information for each type, it charges prices that are equivalent to practising perfect price discrimination on the advertiser side.

**Keywords**: Privacy issues, Information disclosure, Digital media, Monopoly Platform

**JEL Classification**: L12, L86

# 1 Introduction

Online platforms usually generate revenue by providing advertisers with access to data about their user base (Acquisti, Taylor, and Wagman, 2016). There are third-party businesses, such as Acxion and Bloomberge, that exist on the market to enable the collection and trading of data. The most popular technology that data providers use is cookies. When a user visits a data provider's partner website for the first time, a cookie will be sent to the browser and used to record any behaviors of that user on the website. Thus, data providers can collect detailed data on each user and identify their consumption characteristics (Bergemann and Bonatti, 2015). Furthermore, the number of users participating in social networks nowadays is ever-increasing. So social media platforms, such as Facebook and Twitter, are constantly enhancing their interaction effects with users by collecting and analyzing information about users in an attempt to explore more opportunities for profitability. For example, when users share information about their preferences for a product or service on the platform (Kirpalani, and Philippon, 2020), by selling that information to advertisers, platforms can potentially earn more profits since they presumably deliver the most relevant ads to the consumer (Acquisti, Taylor and Wagman, 2016) which provides incentives to users to share more information in the first place. While users can enjoy a personalized social experience on the platform, the collection and use of such personal information may also raise public concerns about privacy issues.

For example, when a person posts an image of her dining at a well-known restaurant on a social media platform, it may reveal information about the preferences of other customers through their "likes" or "dislikes". Or, one's purchasing history and personal information on shopping websites may be resold to third-party companies without one's knowledge. This could lead to one's receiving a large number of spam emails or spam phone calls for some time afterward.

The understanding of the term privacy is not uniformly defined in the relevant fields of study. Research interest in privacy issues generally focuses on the control and protection of personal information, since personal information that can be collected, analyzed, and transacted usually has significant economic values (Acquisti, Taylor and Wagman, 2016). First, users can enjoy direct benefits from sharing information, e.g through saving the time and search costs of getting matched with the most desired advertisements (Kirpalani and Philippon, 2020). Second, the sharing of personal information may create positive or negative externalities because such information can be nonrival. In some cases, users who share their personal information may allow the platform to infer more information about non-users (Choi, Jeon, and Kim, 2019). Users may not know how platforms will deal with their personal data. Therefore, they are likely to be concerned about the various harms caused by the direct or accidental use of data (Lee, Ahn, and Bang, 2011). For example, some studies focus on the relationship between consumer data and price discrimination by retailers. There is no open market for per-

sonal data in which users themselves can participate currently. Therefore, how to protect privacy without diminishing the benefits of sharing information has attracted widespread research interests. The main policy adopted by the platform is to allow users to customize the privacy settings when using the platform (Acquisti, Taylor and Wagman, 2016). For example, access to users' location information can be prohibited when not using the platform's services.

From an economic perspective, the impacts of control and protection of personal information depend on specific contexts (Acquisti, Taylor and Wagman, 2016). For example, users can either reject some terms in the cookies or connect their social media platform with an E-commerce platform (Ichihashi, 2020). The user's decision to share information therefore involves a trade-off between the gain from sharing information and the loss or risk that the user is willing to bear by sharing information. In many cases, users claim to care about privacy while providing excessive information to the platform at the same time, which is known as the privacy paradox (Norberg et al., 2007). Pallant et al. (2022) suggest five factors that influence users' incentives for information sharing, which are value, risk, vulnerability, transparency, and control. Their empirical results suggest that platforms should aim to provide transparency and control over privacy policies since users greatly value these two factors.

This paper aims to provide answers to questions such as what are user's privacy concerns when a user discloses heterogeneous personal information

on the social media monopoly, and what are the effects of user's different concerns on the social media platform's profitability when considering a trading market of user $i$'s personal information? In our paper, when a certain user joins a social media platform, she will disclose two different types of personal information. The first type of information reveals the user's personal identity, such as name, email address, hobbies etc., which are mainly used to create a personal profile. The second type of information reveals the user's other characteristics such as shopping preferences and similar behaviors. Then the user's privacy concern under each type of information will be different. In our paper, the user's privacy concern arises due to the user's willingness to disclose a certain amount of each type of personal information (instead of the accuracy of personal information disclosed). Then, under each type of information, users face a trade-off between privacy benefits and privacy risks. Upon collecting information from the users, the platform needs to process and protect such information which normally requires a substantial amount of investment on the platform's part. The platform also provides a separate trading service to the advertiser by deciding on both the amounts o be traded for each type of information and the corresponding prices to be charged for each type of sale. The advertiser in our model plays a passive role: he only decides whether to receive the trading service after observing the platform's decision.

Our results highlight that the user's information disclosure strategies are quite different when they face different types of privacy concerns. Faced with

the privacy concern of cybersecurity risks such as cyberbullying attacks, users behave cautiously about disclosing information that reveals their personal identities. However, faced with privacy concerns of preference information breaches, users behave less cautiously whereby they always disclose a certain amount of information on the platform.

The remaining sections are structured as follows. Section 2 reviews related literature. Section 3 provides the basic model setting. Section 4 discusses user's privacy concerns with equilibrium outcomes. Section 5 concludes. All proofs are in the Appendix.

# 2 Literature Review

Few studies have discussed consumers' willingness to provide marketers with different types of personal data. Phelps, Nowak, and Ferrell (2009) focused on consumers' attention to information-behavioral consistency and their perceptions of exchange relationships with marketers who collect and use personal information. Specifically, consumers' overall concerns about how companies use their personal information depend on four general factors: (1) the type of personal information requested, (2) the amount of control over the information provided, (3) the potential exchange offerings, consequences, and benefits, and (4) consumer characteristics. Both consumers and marketers often look at privacy issues in terms of information control – i.e. control over who has access to personal data (i.e. disclosure), how personal data is used

(i.e. misappropriation and fake light), and the amount of advertising and marketing offers coming from use (i.e. hacking) of personal data. A high degree of information control means that consumers can meaningfully influence the use of information about them. Two key underlying assumptions are: (1) most consumers want more control and (2) giving consumers more control over how information about them is used will alleviate their privacy concerns.

For the platform, protecting users' data from malicious third parties is often costly. In addition, the platform should also decide on the extent to which it should maintain privacy protection. For example, Google and Apple have already developed privacy protection tools to restrict data freely flowing to other parties (Goldfarb and Que, 2023). From a public policy perspective, the most important factors are the type of information collected and the degree of consumer control over subsequent dissemination. This research will analyze a theoretical model to examine the relationship between user's privacy concerns and the degree of control provided by the platform.

Since misuse of information is a particularly prominent form of online risk and respect for privacy is often closely associated with trust in consumer surveys, building consumer trust is a valuable way for platforms to encourage consumers to disclose personal data. Lutz (2018) also developed and tested a framework for analyzing the impact of privacy concerns on sharing that considers institutional and societal privacy threats, trust, and social and monetary motives. User trust, such as classifying a particular service

provider as trustworthy, will allow users to rely on their services and enjoy their benefits without the need for complex risk calculations or extensive protective actions. A well-documented heuristic for forming trust beliefs is based on fair information practices (i.e. proactive communication of security and privacy policies, assurances and further customer service). Similarly, according to Martin (2018), consumers find that breaches of privacy expectations, especially secondary use of information, reduce trust in websites. Companies that violate privacy expectations are penalized twice: once through privacy violations directly affecting consumers' trust; and through the (perceived) reductions of the importance of trust factors such as integrity and competence to trust. Trust therefore mitigates privacy concerns by removing the risk of misuse of information, thereby highlighting the importance of building trust in maintaining online consumer relationships. Consumers are able to make trust judgments regardless of the content of the privacy statement. Potential competitive advantages can be achieved by respecting privacy, increasing trust, and placing greater emphasis on a company's competence and integrity. In our research, consumers' trust in the platform will depend upon the effect of the degree of control exercised by the platform which will then affect the user's decision on data sharing.

Information externalities, positive or negative, usually arise when users share data on social media platforms. This creates a series of interconnected effects: First, a certain user's interactions with other users can reveal his or her connections. Consequently, other people's preferences can be revealed

through their interactions with the current user. Finally, all users' behaviors in other markets, such as online shopping, are also revealed through the information they may share on the platform (Goldfarb and Que, 2023). Choi, Jeon and Kim (2019) considered indirect information externalities and discussed a theoretical model of privacy in which data collection requires consumer consent, and consumers are fully aware of the consequences of such consent. Nonetheless, excessive collection of personal information occurs in monopolistic market equilibrium, which leads to an excessive loss of privacy compared to the social optimum. The main mechanisms for this outcome are information externalities and user coordination failures, some of whom decide to share their personal information which may allow data controllers to infer more information about non-users. However, they specify that information is heterogenous from the perspective of information externalities, and lack of research on the role of policy on privacy control. Acemoglu et al. (2022) also consider a monopoly market where the platform can trade data. They find that excessive use of data by the platform will lead to negative externalities and therefore the data will be underpriced which may not affect consumer's valuation of privacy.

Acquisti, Taylor, and Wagman (2016) considered an economic analysis of privacy issues and showed that based on different theories and evidence, privacy protection can either increase or decrease welfare. In addition, the definition of privacy also depends on different situations, so the trade-offs of sharing personal data should be discussed specifically. According to previous

studies, firms usually protect consumers' data when consumers realize how the firm can benefit from their data so that they may change their purchasing decisions. Sometimes firms can also gain more benefits under privacy protection behaviors. As the intermediaries of sharing data, such as Google and Facebook, they may provide relevant services on one side and sell advertisement positions on the other side. When users on one side open their personal data to the platform, they will usually be matched with more relevant advertisements, whilst for those who completely hide their data, the content of an advertisement is likely to be random. Furthermore, the study also reviewed a monopoly data-sharing platform with heterogeneous consumers on one side and advertisers on the other side. By comparing situations under complete information, they show that the platform and advertisers may not achieve a socially optimal match, when the advertisers acquire only part of the information. Bergemann and Bonatti (2015) also studied transactions between the platform and the advertisers. Their result shows that direct data sharing to advertisers can lead to a decrease of advertisement purchasing positions on the advertiser side so the platform will limit the accuracy of shared data to make profits.

Taylor and Wagman (2014) discussed several models under the oligopoly market with firms and consumers to compare the profit maximization and social welfare issues under the privacy and non-privacy contexts. In linear city and circular city models, firms set uniform prices under a privacy context, in which firms have no information about consumers. Firms set prices

based entirely on consumer types in a non-privacy context in which consumer information is common knowledge. Their results showed that consumers are better off without privacy. In a vertical differentiation model, two firms are differentiated by quality, and consumers are differentiated by their willingness to pay. The result shows that consumers with a higher willingness to pay would prefer privacy and more consumers would choose high-quality firms without privacy. In a multi-unit symmetric demand model, firms set pricing strategies with complementary features. Compared to the privacy context, consumer surplus and social welfare are both reduced under the non-privacy context, although the profits were higher. Therefore, the effect of privacy enforcement should be considered under the specific economic model.

Duan, Liu, and Feng (2022) study pricing strategies in online platforms based on privacy concerns. The online platform provides original new content, charges a subscription price on the user side, provides users' information to improve the targeting level in online advertising, and charges a price for the advertising slot on the advertiser side. The analysis shows that the platform's pricing decisions depend on the level of information disclosure, and when the information disclosure is at an intermediate level, the maximum surplus can be achieved. Ichihashi (2023) introduced a dynamic model of consumers' privacy choices on the platform. The study highlights the platform's information collection strategies through a commitment to not collect a great amount of information in the early period. As a result, consumers are more willing to use the platform's services. Fainmesser, Galeotti and Momot

(2023) theoretically measured the effect of data protection regulations. Their result shows that social efficiency will be satisfied if the authority imposes policies of combining minimum data protection levels with taxes or fines.

Our paper contributes to the literature on privacy concerns issues in two-sided markets in a novel way. Whilst the previous literature has discussed the role of privacy concerns on a platform's decision to monetize user's information, the research question in our paper focuses on how users' trade-off between different types of information disclosure decisions affect a platform's strategic decision about what type of information and how much information to be traded and prices to be charged in the trading market. Our model specifically considers the trade-offs between different types of information to be disclosed. By disclosing personal information about personal identities, whilst the users will enjoy positive network effects among a vast size of users, they will also be subjected to the risk of being exposed to attacks of cyberbullying and reputation damage. Whilst the user will experience better matching of advertisers' products by disclosing personal information about shopping preferences and behaviors, they may also be subjected to the nuisance cost due to the information breach to the advertiser.

# 3 Model Setup

Consider a market with a monopoly social media platform, a mass one of Internet users, and an advertiser.

## 3.1 Users

Internet users' valuation of the platform service is uniformly distributed over $[\underline{v}, \bar{v}]$, with a distribution function $F$. Then the mass of users who join the platform is measured by $1 - F(\underline{v})$. When users join the platform, they do not pay any subscription fees but should provide a certain amount of personal information to create an account, such as user names, email addresses, gender information, etc. Users can share more such personal information of this type by e.g. adding their interests and hobbies on their personal profiles, posting a selfie picture, and clicking the "like" button on others' comments. Such information, when shared on the platform, can provide users with further personalized and targeted services. We call this type of information as type 1 information. On the other hand, a user can also share certain other personal information such as her shopping preferences and related behaviour. We call this type 2 information.

Suppose user $i$ joins the platform and can potentially disclose two types of personal information, type 1 and type 2. By disclosing type 1 personal information, user $i$ can enjoy network effects from interacting with other users. In a traditional two-sided market analysis, an agent's network effect enjoyed on one side usually relates to the number of agents on the other side. Our model assumes that such network externalities arise on the *same* side of the market since, depending on the mass of users, a certain user can enjoy interaction utilities with other like-minded users who have found this particular platform's characteristics more suitable to their tastes. Hence, if

user $i$ chooses $x_1$ amount of type 1 information to disclose, her social network utility on the user side is given by $x_1\alpha[1-F(\underline{v})]$, where $\alpha > 0$ is the network effect parameter. At the same time, user $i$ may also be exposed to potential cybersecurity risks, such as identity theft and cyberbullying attacks. Denote this cybersecurity risk parameter by $s(s > 0)$. Then user $i$'s privacy cost of disclosing $x_1$ amount of type 1 information is given by $x_1 s[1-F(\underline{v})]$. User $i$'s privacy cost of disclosing type 1 personal information relies on both the amount of information disclosed and the mass of users on the platform. That is, disclosing more specific personal information on a relatively popular social media platform will increase the risk of being exposed to cyberbullying attacks. To make our analysis tractable, we assume that user $i$'s utility of disclosing $x_1$ amount of type 1 information is defined in the following form:

$$u_i(x_1) = x_1(\alpha - s)[1-F(\underline{v})] - \frac{1}{2}x_1^2 \tag{1}$$

where the first term implies that if the cybersecurity risk $s$ is higher than the positive network effect $\alpha$, i.e. if $\alpha < s$ then the net effect of interacting with other users will be negative and will lead to a disutility of disclosing type 1 information. The second term represents the privacy cost of disclosing $x_1$ amount of type 1 information.[1]

In contrast, type 2 information mainly reveals user $i$'s shopping preferences and similar behaviors. Thus, by disclosing personal information of the

[1]See our analysis in section 4.3 and after, for the user's decision to disclose $x_1$ and its implications.

type 2 category, user $i$ can enjoy the benefits of targeted service. For example, by analyzing information disclosed by user $i$, the platform can match user $i$ to a product of the advertiser that is more suitable to user $i$. If user $i$ chooses $x_2$ amount of type 2 information to disclose, her utility of being matched to the advertiser is given by $mx_2$, where the parameter $m > 0$ represents the matching benefit. At the same time though, the user $i$ may also be exposed to potential risks. For example, if user $i$'s private information about his willingness to pay for a specific good is breached (e.g. by the platform to the advertiser), she may then suffer price discrimination from the advertiser. User $i$'s privacy cost of disclosing $x_2$ amount of type 2 information is also defined as a quadratic function $\frac{1}{2}\phi x_2^2$, where $\phi > 0$ is the nuisance cost parameter. Therefore, the net utility of user $i$ for disclosing $x_2$ amount of type 2 information is:

$$u_i(x_2) = mx_2 - \frac{1}{2}\phi x_2^2 \tag{2}$$

Thus, user $i$'s total utility function of disclosing both types of information is written as

$$u_i = x_1[\alpha - s][1 - F(\underline{v})]] - \frac{1}{2}x_1^2 + mx_2 - \frac{1}{2}\phi x_2^2 \tag{3}$$

## 3.2 The Monopoly Platform

The monopoly platform collects all the amount of information $\{x_1, x_2\}$ disclosed by user $i$. Holding user's personal information is usually very costly for the platform because the information management system requires a high

level of investment. Therefore, trading user's information can help reduce the platform's holding cost. The platform can therefore decide whether to trade a certain amount of information with the advertiser. Suppose the platform charges a price $p_1$ on each unit of type 1 information and a price $p_2$ on each unit of type 2 information. Besides setting the prices, the platform also chooses a fraction $\gamma_1$ of $x_1$ amount of type 1 information and a fraction $\gamma_2$ of $x_2$ amount of type 2 information to trade, $\gamma_1, \gamma_2 \in [0, 1]$.[2] Thus, the platform's total revenue of trading user $i$'s personal information is $p_1\gamma_1 x_1 + p_2\gamma_2 x_2$.

Suppose that $c_1$ is the cost of holding each unit of type 1 information collected, and $c_2$ is the cost of holding each unit of type 2 information collected, $c_1, c_2 > 0$. Then the total holding cost of keeping non-traded information is $c_1(1-\gamma_1)x_1 + c_2(1-\gamma_2)x_2$. Thus, the total payoff function of the platform for trading user $i$'s information is written as

$$\pi_P = [p_1\gamma_1 x_1 - c_1(1-\gamma_1)x_1] + [p_2\gamma_2 x_2 - c_2(1-\gamma_2)x_2] \tag{4}$$

where the first two terms represent the net payoff from trading $\gamma_1 x_1$ amount of type 1 information, and the last two terms represent the net payoff from trading $\gamma_2 x_2$ amount of type 2 information.

[2]Without any loss of generality, we assume the trading cost to be zero.

## 3.3 The Advertiser

In this model, the advertiser plays a relatively passive role. Without buying user $i$'s information, the advertiser could only build an official social presence, display a certain amount of basic information about all products on the platform, and connect with the user $i$ through the platform's matching service. However, if the advertiser buys user $i$'s information from the platform, it can generate separate target capabilities as both types of user $i$'s information can be analyzed and identified as possible targeting options. Thus, the advertiser can enjoy further benefits such as increased revenues from selling user $i$ a specific product. Denote the benefit enjoyed from buying each unit of user $i$'s type 1 information by $b_1$, and the benefit enjoyed from buying each unit of user $i$'s type 2 information by $b_2$, where $b_i > 0$ $i = 1, 2$. We assume that the information processing cost for the advertiser is quadratic so that $\frac{1}{2}(\gamma_i x_i)^2$ denotes the cost of processing $\gamma_i x_i$, $i = 1, 2$ amount of users' type $i, i = 1, 2$ information, that has been purchased from the platform. Then, the total utility function of the advertiser from buying user $i$'s information can be defined as a quadratic form:

$$u_A = [(b_1 - p_1)\gamma_1 x_1 - \frac{1}{2}(\gamma_1 x_1)^2] + [(b_2 - p_2)\gamma_2 x_2 - \frac{1}{2}(\gamma_2 x_2)^2] \qquad (5)$$

where the first two terms capture the advertiser's net utility of buying user $i$'s type 1 information, and the last two terms capture the net utility of buying user $i$'s type 2 information.

### 3.4 Stages of the game

The following analysis will be based on user $i$'s disclosure strategies and the platform's trading strategies. Specifically, the timing of the game is as follows.

- **Stage 1**: User $i$ joins the platform and decides how much of type 1 information $x_1$, to disclose, and how much type 2 information $x_2$ to disclose if she joins.
- **Stage 2**: The platform collects user $i$'s disclosed information $\{x_1, x_2\}$ and decides on the proportion of user $i$'s each type of information $\gamma_i$ to trade and the corresponding price $p_i$ to charge, $i = 1, 2$.
- **Stage 3**: The advertiser observes the platform's decisions $\{p_1, \gamma_1, p_2, \gamma_2\}$ and decides whether to buy user $i$'s personal information.

## 4 Equilibrium Analysis

The game will be solved by backward induction.

### 4.1 Advertiser's Purchasing Decision

At stage 3, the advertiser purchases user $i$'s information if and only if his total utility from doing so (weakly) exceeds his reservation utility level which is obtained from providing some basic information on the platform (i.e. before buying any further information from the platform) which we, for simplicity

and without any loss of generality, normalise to zero. Hence, the individual rationality (henceforth IR) condition of the advertiser with respect to its purchasing behavior is given as below:

$$[(b_1 - p_1)\gamma_1 x_1 - \frac{1}{2}(\gamma_1 x_1)^2] + [(b_2 - p_2)\gamma_2 x_2 - \frac{1}{2}(\gamma_2 x_2)^2] \geq 0 \tag{6}$$

First of all, note that if both $\gamma_1 = 0$ and $\gamma_2 = 0$, when $x_i \geq 0$, $i = 1, 2$ i.e. when the platform decides to sell no information to the advertiser, despite the fact that the user has provided $x_i$ on the platform, it makes no profits. Therefore, to have a meaningful analysis, we focus on the other possible cases where at least one of the $\gamma_i x_i$s is positive as described below.[3]

(1) If $\gamma_1 x_1 > 0$ and $\gamma_2 x_2 = 0$, then the IR condition of the advertiser as given by equation (6) reduces to,

$$(b_1 - p_1)\gamma_1 x_1 - \frac{1}{2}(\gamma_1 x_1)^2 \geq 0 \tag{7}$$

implying that the advertiser must receive non-negative utility from purchasing the type 1 information as no type 2 information is provided by the platform. The above then implies that the advertiser will purchase user $i$'s type

[3]However, note that the platform's decisions to sell either or both types of information depend upon the users' decision to provide such information. We, therefore, assume, for the time being, that the users decide to provide at least one category of information. Also see our analysis in Section 4.3.

1 information if and only if the following holds

$$b_1 \geq p_1 + \frac{1}{2}\gamma x_1 \tag{8}$$

Similarly,

(2) If $\gamma_1 x_1 = 0$ and $\gamma_2 x_2 > 0$, then the IR condition of the advertiser reduces to,

$$(b_2 - p_2)\gamma_2 x_2 - \frac{1}{2}(\gamma_2 x_2)^2 > 0 \tag{9}$$

implying that the advertiser must now receive non-negative utility from purchasing the type 2 information since no type 1 information is provided by the platform i.e the advertiser purchases user $i$'s type 2 information if and only if

$$b_2 \geq p_2 + \frac{1}{2}\gamma_2 x_2 \tag{10}$$

(3) If both $\gamma_1 x_1 > 0$ and $\gamma_2 x_2 > 0$ hold, then the advertiser will purchase user $i$'s information as long as its individual rationality condition is satisfied as given by equation (6).

## 4.2 The Platform's Trading Decision

In stage 2, the platform chooses the proportions $\gamma_i, i = 1, 2$ of each type of information to trade and the corresponding prices $p_i, i = 1, 2$ to charge, to maximise its profits. We assume $b_i > c_i$ so that trading in information of type $i$ is feasible. The platform's optimization problem can now be defined

as

$$\max_{\gamma_1,\gamma_2,p_1,p_2} \pi_P = [p_1\gamma_1 x_1 - c_1(1-\gamma_1)x_1] + [p_2\gamma_2 x_2 - c_2(1-\gamma_2)x_2] \tag{11}$$

s.t.

$$[(b_1 - p_1)\gamma_1 x_1 - \frac{1}{2}(\gamma_1 x_1)^2] + [(b_2 - p_2)\gamma_2 x_2 - \frac{1}{2}(\gamma_2 x_2)^2] \geq 0 \tag{12}$$

By solving the optimization problem, the following proposition is obtained.

**Proposition 1** *The monopoly platform will not make any trading decisions on either type of information if users disclose nothing about their types. If user i only discloses type 1 information, then the monopoly platform's profit is maximized by the solution* $\{\gamma_1^*, p_1^*\}$ *where* $\gamma_1^* = \frac{b_1+c_1}{x_1}$, $p_1^* = \frac{b_1-c_1}{2}$. *If user i only discloses type 2 information, then the monopoly platform's profit is maximized by the solution* $\{\gamma_2^*, p_2^*\}$ *where* $\gamma_2^* = \frac{b_2+c_2}{x_2}$, $p_2^* = \frac{b_2-c_2}{2}$. *If user i discloses both type 1 and type 2 information, then the monopoly platform's profit is maximized by the solution* $\{\gamma_1^*, p_1^*, \gamma_2^*, p_2^*\}$ *that* $\gamma_1^* = \frac{b_1+c_1}{x_1}$, $p_1^* = \frac{b_1-c_1}{2}$, $\gamma_2^* = \frac{b_2+c_2}{x_2}$, $p_2^* = \frac{b_2-c_2}{2}$.

**Proof**: See the Appendix.

The implication of Proposition 1 is as follows. The platform's trading decision is made by observing user $i$'s disclosure choice. The platform's profit can be maximized only when at least one type of personal information is disclosed by user $i$. Note that regardless of whether the platform trades only one type of information or both, the functional forms for the optimal values

of $\gamma_i$ and $p_i$ remain the same although the actual equilibrium values will differ depending upon the equilibrium values of $x_i$ that are decided by the users (see the analysis in the next sub-section). When the platform collects a certain amount of information of either type, the optimal traded fraction of each type of information is determined by the advertiser's marginal benefit enjoyed from purchasing that type of information, the platform's marginal cost of holding that type of collected information, and user $i$'s disclosed level of that type of information. For example, for the type 1 information $x_1$ collected, either a higher marginal benefit enjoyed by the advertiser $b_1$, or a higher marginal holding cost $c_1$ undertaken by the platform will increase the traded volume of type 1 information $\gamma_1^* x_1$. Similarly, for type 2 information $x_2$ collected: either a higher value of $b_2$ or $c_2$ or both will increase the traded volume of type 2 information $\gamma_2^* x_2$. Therefore, when holding user $i$'s personal information is costly, the platform always has an incentive to increase the traded proportion of user $i$'s personal information.

The optimal price levels charged for each type of information are determined by the advertiser's marginal benefit enjoyed from purchasing each type of information and the platform's marginal cost of protecting that type of information. Note that the prices $p_i^*, i = 1, 2$ are strictly positive since $b_i > c_i$. Indeed, for given values of $c_1$ and $c_2$, higher the values of $b_1$ and $b_2$, higher will be the equilibrium price levels $\{p_1^*, p_2^*\}$ charged by the platform: The platform has a significant advantage in terms of user $i$'s information that advertiser requires, so it will practice perfect price discrimination when it

has complete information of the advertiser's willingness to pay. That is, the platform charges a higher price and trades a higher volume of information of a certain type for which the advertiser's benefit is higher. On the contrary, for higher values of $c_1$ and $c_2$, the platform will choose lower values of equilibrium price levels $\{p_1^*, p_2^*\}$. A higher per-unit holding cost of a specific type of information can lead to a higher traded amount of information of that type, which will significantly reduce the platform's total holding cost of that type's collected information. Therefore, this may allow the platform to maintain its profitability by charging a lower price.

For $\gamma_2^* \geq 0$ and $\gamma_2^* \geq 0$, i.e. when $x_1 > 0$ and $x_2 > 0$, the platform's maximized profit is given by

$$\pi_P^* = [\frac{(b_1 + c_1)^2}{2} - c_1 x_1] + [\frac{(b_2 + c_2)^2}{2} - c_2 x_2] \tag{13}$$

The first term captures the platform's maximized profit from trading user $i$'s type 1 information, and the second term captures the platform's maximized profit from trading user $i$'s type 2 information. Each term shows how traded information offsets the holding cost of the total amount of each type of information. The platform therefore makes non-negative profits whenever the following holds:

$$c_1 x_1 + c_2 x_2 \leq \frac{(b_1 + c_1)^2}{2} + \frac{(b_2 + c_2)^2}{2} \tag{14}$$

Note that at the optimal solution, the advertiser's utility is zero ($u_A^* = 0$

as the IR binds) which implies perfect price discrimination exercised by the platform as by charging different prices for different categories of information, the platform fully extracts all surpluses generated from each category of information, from the advertiser.

## 4.3 The User's Disclosure Decision

At stage 1, user $i$ chooses the optimal disclosure level of type 1 and type 2 information by solving the following utility maximization problem.

$$\max_{x_1,x_2} u_i = x_1(\alpha - s)[1 - F(\underline{v})] - \frac{1}{2}x_1^2 + mx_2 - \frac{1}{2}\phi x_2^2 \tag{15}$$

Proposition 2 characterizes the optimal solution.

**Proposition 2** *With privacy concerns for both type 1 and type 2 information, the optimal values of $x_1^*$ and $x_1^*$ that maximize user $i$'s utility are given by*

$$x_1^* = (\alpha - s)[1 - F(\underline{v})] \tag{16}$$

*if and only if $\alpha \geq s$, and*

$$x_2^* = \frac{m}{\phi} \tag{17}$$

The implication of Proposition 2 is as follows. For $x_1^* \geq 0$ to hold, $\alpha \geq s$ must hold. User $i$'s optimal disclosure level of type 1 information is determined by the extent of marginal net externalities obtained from interacting with other users on the user side. If marginal net externalities of interacting

with other users are non-positive, so that $\alpha \leq s$, then disclosing type 1 information will generate disutilities. On the other hand, if the net externalities of interacting with other users on the user side are sufficiently positive, then user $i$ will disclose type 1 information as much as possible to realize as much network utilities as possible.

In contrast, $x_2^*$ is *always* positive implying that user $i$ is always willing to disclose a certain amount of type 2 information. User $i$'s optimal disclosure level of type 2 information is determined by $m = \phi x_2^*$. The left-hand side captures the marginal benefit enjoyed from being matched with the advertiser, while the right-hand side captures the marginal privacy cost of disclosing type 2 information. With $\phi$ fixed, the higher the value of matching benefits user $i$ enjoys, the higher the disclosure level of type 2 information the agent chooses. If on the other hand, with $m$ fixed, a higher value of $\phi$ implies that the user $i$ will choose to disclose a lower level of type 2 information. User $i$ knows the platform may disclose her type 2 information to achieve more targeted advertising, but she does not know exactly how much of type 2 information will be breached. So if user $i$ behaves naively and has fewer privacy concerns, she will disclose type 2 information as much as possible. On the other hand, if user $i$ is cautious and feels sensitive about the information breach, she may still disclose type 2 information but will likely disclose a relatively small level of information. Therefore, user $i$'s privacy concerns of disclosing type 2 information rely both on the matching performance with the advertiser and her attitudes toward information breach.

With the above optimal solution, for $\alpha \geq s$, user $i$'s total utility is presented by

$$u_i^* = \frac{1}{2}(\alpha - s)^2[1 - F(\underline{v})]^2 + \frac{1}{2}\frac{m^2}{\phi} \tag{18}$$

The above implies that in equilibrium the user $i$ chooses to reveal a combination of $x_2^*$ and $x_1^*$ such that she receives (net) positive utility from being operative on the platform: even if the user $i$ generates zero net utilities from disclosing type 1 information, she can still receive positive payoff by disclosing type 2 information.

With the optimal solution of $x_1^* > 0$, $x_2^* > 0$, platform's optimal traded fraction $\{\gamma_1^*, \gamma_2^*\}$ is written as

$$\gamma_1^* = \frac{b_1 + c_1}{(\alpha - s)[1 - F(\underline{v})]} \tag{19}$$

$$\gamma_2^* = \frac{\phi(b_2 + c_2)}{m} \tag{20}$$

The conditions of $\gamma_1^*, \gamma_2^* \in [0, 1]$ are given by

$$\alpha - s > 0 \tag{21}$$

$$b_1 + c_1 \leq (\alpha - s)[1 - F(\underline{v})] \tag{22}$$

$$b_2 + c_2 \leq \frac{m}{\phi} \tag{23}$$

The above results imply that, when user $i$ reveals type 1 information (i.e.

when $\alpha - s > 0$), the platform trades a positive amount of type 1 information whenever user $i$'s marginal utility of disclosing type 1 information is (weakly) greater than the sum of platform's marginal cost of holding type 1 information and the advertiser's marginal benefit of purchasing type 1 information (inequality (22)). Inequality (23) implies that when the platform trades a positive amount of type 2 information, the disclosed level of type 2 information is always greater than the sum of the platform's marginal cost of holding type 2 information and the advertiser's marginal benefit of purchasing type 2 information.

The platform's maximized profit $\pi_P^*$ is written as

$$\pi_P^* = \{\frac{(b_1 + c_1)^2}{2} - c_1(\alpha - s)[1 - F(\underline{v})]\} + \{\frac{(b_2 + c_2)^2}{2} - \frac{c_2 m}{\phi}\} \qquad (24)$$

**Proposition 3** *Keeping other things fixed, higher values of holding cost* $\{c_1, c_2\}$ *will lead to a lower profit of platform* $\pi_P^*$.

**Proof:** See the Appendix.

The implication of Proposition 3 is as follows. The platform's profitability from trading user $i$'s collected information of each type reflects a trade-off between the platform's holding cost and its service performance on both sides. When the platform has to invest a large amount for holding user $i$'s personal information, the total benefits of collecting and purchasing information may not offset the holding cost which then will have a negative effect platform's profitability.

**Proposition 4** *Keeping other things fixed, higher values of $\phi$ lead both to a higher proportion of type 2 information $\gamma_2^*$ being traded as well as to higher platform profits $\pi_P^*$.*

**Proof:** See the Appendix.

Proposition 4 can be explained as follows. The privacy cost of user $i$ for disclosing $x_2^*$ amount of type 2 information is $\frac{1}{2}\phi x_2^{*2} = \frac{1}{2}\frac{m^2}{\phi}$. When $\phi$ increases, the equilibrium value of user $i$'s privacy costs for this type of information actually decreases adding to an increased value of net utilities (see equation (18)). Thus, user $i$ will be willing to disclose a higher level of type 2 information. When the platform observes user $i$'s disclosure level, it increases the traded fraction of $\gamma_2$ to maintain a higher profitability.

**Proposition 5** *Keeping other things fixed, a higher value of $s$ leads to higher profits $\pi_P^*$ for the platform.*

**Proof:** Straight-forward differentiation of the profit expression $\pi_P^*$ (given by equation (24)) with respect to $s$ yields the result: $\frac{\partial \pi_P^*}{\partial s} = c_1 > 0$. QED.

When $s$ becomes higher (but still lower than $\alpha$), user $i$ will have increased privacy concerns for cybersecurity risk and, therefore, will disclose less type 1 information. This also leads to a lower cost of holding user $i$'s type 1 information. Thus, the platform's profit will be higher.

## 4.4 Potential Privacy Protection and some Implications for Regulations

The equilibrium results above show different information disclosure decisions of Internet users when faced with two types of personal information that can potentially be disclosed, which further affect the platform's trading choices. Specifically, Internet users respond more sensitively while disclosing type 1 information. When the platform wants to make profits from trading both type 1 and type 2 information, it (possibly) tries to keep the user's privacy concern of cybersecurity risk under control. One feasible solution that can be analyzed further is that for the platform to commit to not sharing any type 1 information i.e. the platform should promise to share only type 2 information with other parties such as advertising bodies. Another feasible solution can be to have government intervention in the market to ensure the protection of privacy rights and fairness of information sharing. For example, the European Commission introduced the Digital Service Act and the Digital Market Act in 2020 to protect consumer's fundamental rights on digital platforms, which can provide users with a better cybersecurity environment.

# 5 Conclusion

This paper analyzes the role of Internet users' privacy concerns in a monopoly social-media platform, where users can interact with other users and can

potentially get matched with advertising bodies. Platforms provide such matching services by collecting information from the users and trading some of the collected information with the advertisers, in most cases, without the users' knowledge. In our paper, we consider two types of privacy concerns by the user. The first type of privacy concern is related to the user's disclosure choice of certain personal information that can also create network effects on the user side. The disclosure decision is determined by interactions between benefits enjoyed and the potential for facing cyber-security risks. The equilibrium disclosure level is determined by weighing these two aspects. The second type of privacy concern is related to the user's disclosure choice of information which can generate matching benefits through getting matched with the right advertiser. We find that in equilibrium, this disclosure decision is determined by weighing matching benefits with the nuisance cost of an information breach. Specifically, the equilibrium level of information is such that the marginal matching benefit equals to marginal privacy cost. The monopoly platform collects both types of user information and decides whether to trade a certain amount of each type with the advertiser and how much to charge for each category of information.

Our results imply that the platform practices perfect price discrimination on the advertiser side, which generates zero utility for them from trading information. Differences in the equilibrium price levels charged for each type of information traded rely on the advertiser's marginal benefit of purchasing each type of information and the platform's marginal cost of holding that

type of information. Comparing users' privacy concerns under two different types of personal information, we find that the user behaves more cautiously in disclosing type 1 (i.e. personal identity related) information than disclosing type 2 (e.g. shopping behaviour related) information: Whilst the user may not disclose any (additional) type 1 information if she believes that the risk of cybersecurity is high, she will always disclose type 2 information even with privacy concerns of an information breach. Our results explain how information holding costs affect the platform's profitability. Whilst high holding costs always increase the platform's incentives to trade users' personal information more, it may also reduce the platform's profitability because the total benefits of collecting and purchasing information may not be offset by the information holding cost.

It would be interesting to explore the role of user privacy concerns further in the context of other market configurations. For example, the monopoly platform framework can be extended to an oligopolistic setting. Each platform will then compete for collecting user's information on one side while competing for advertisers to trade users' information on the other side. Such extensions remain in our future research plans.

# Appendix

## A Proofs of the Main Results

### A.1 Proof of Proposition 1

**Proof.** The Lagrange function $L$ for the maximisation problem is given as below, where $\lambda$ represents the Kunh-Tucker multiplier.

$$\begin{aligned} L =&[p_1\gamma_1 x_1 - c_1(1-\gamma_1)x_1] + [p_2\gamma_2 x_2 - c_2(1-\gamma_2)x_2] \\ &+\lambda[(b_1-p_1)\gamma_1 x_1 - \frac{1}{2}(\gamma_1 x_1)^2 + (b_2-p_2)\gamma_2 x_2 - \frac{1}{2}(\gamma_2 x_2)^2] \end{aligned} \tag{25}$$

The Kuhn-Tucker conditions are:

$$\frac{\partial L}{\partial \gamma_1} = p_1 x_1 + c_1 x_1 + \lambda[(b_1-p_1)x_1 - \gamma_1 x_1^2] \leq 0, \gamma_1 \geq 0 \tag{26}$$

$$\frac{\partial L}{\partial \gamma_2} = p_2 x_2 + c_2 x_2 + \lambda[(b_2-p_2)x_2 - \gamma_2 x_2^2] \leq 0, \gamma_2 \geq 0 \tag{27}$$

Since the platform's profits are monotonically increasing in prices when $\gamma_i$s are positive, $p_i$s must be positive. Therefore, we have,

$$\frac{\partial L}{\partial p_1} = \gamma_1 x_1 - \lambda\gamma_1 x_1 = 0 \tag{28}$$

$$\frac{\partial L}{\partial p_2} = \gamma_2 x_2 - \lambda\gamma_2 x_2 = 0 \tag{29}$$

$$\frac{\partial L}{\partial \lambda} = (b_1 - p_1)\gamma_1 x_1 - \frac{1}{2}(\gamma_1 x_1)^2 + (b_2 - p_2)\gamma_2 x_2 - \frac{1}{2}(\gamma_2 x_2)^2 = 0 \qquad (30)$$

We consider the following cases:

**Case 1:** $x_1 = 0$ and $x_2 > 0$. In this case, $\gamma_1 = 0$ and $p_1 = 0$ by default. Then the Kuhn-Tucker conditions can be simplified as

$$\begin{aligned} & p_2 + c_2 + \lambda(b_2 - p_2 - \gamma_2 x_2) \leq 0, \gamma_2 \geq 0 \\ & \gamma_2(1 - \lambda) = 0 \\ & (b_2 - p_2)\gamma_2 - \frac{1}{2}\gamma_2^2 x_2 = 0 \end{aligned} \qquad (31)$$

In this case, $\gamma_2$ must be positive, otherwise the platform makes no profit. Since $\gamma_2 > 0$, $p_2$ must be positive. Hence equation (31) implies $\lambda = 1$, and consequently $\gamma_2^* = \frac{b_2 + c_2}{x_2}$ and $p_2^* = \frac{b_2 - c_2}{2}$.

**Case 2:** $x_1 > 0$ and $x_2 = 0$. Similar to case 1, here too, the platform will set neither $\gamma_2$ nor $p_2$ i.e. $\gamma_2 = 0$ and $p_2 = 0$ by default. Then the Kuhn-Tucker conditions can be simplified as

$$\begin{aligned} & p_1 + c_1 + \lambda(b_1 - p_1 - \gamma_1 x_1) \leq 0, \gamma_1 \geq 0 \\ & \gamma_1(1 - \lambda) = 0 \\ & (b_1 - p_1)\gamma_1 - \frac{1}{2}\gamma_1^2 x_1 = 0 \end{aligned} \qquad (32)$$

In this case, too, $\gamma_1$ must be positive, otherwise, the platform makes no profit. Since $\gamma_1 > 0$, hence, $p_1$ must be positive. The Kuhn-Tucker conditions then imply $\lambda = 1$, $\gamma_1^* = \frac{b_1 + c_1}{x_1}$ and $p_1^* = \frac{b_1 - c_1}{2}$.

**Case 3:** $x_1 > 0$ and $x_2 > 0$. If $x_1 > 0$ and $x_2 > 0$, then the Kuhn-Tucker conditions can be simplified as

$$\begin{aligned}
&p_1 + c_1 + \lambda(b_1 - p_1 - \gamma_1 x_1) \leq 0, \gamma_1 \geq 0 \\
&p_2 + c_2 + \lambda(b_2 - p_2 - \gamma_2 x_2) \leq 0, \gamma_2 \geq 0 \\
&\gamma_1(1 - \lambda) = 0 \\
&\gamma_2(1 - \lambda) = 0 \\
&(b_1 - p_1)\gamma_1 - \frac{1}{2}\gamma_1^2 x_1 + (b_2 - p_2)\gamma_2 - \frac{1}{2}\gamma_2^2 x_2 = 0
\end{aligned} \tag{33}$$

Similar to above, $\gamma_1 = 0$ or $\gamma_2 = 0$ cannot hold in this case. Indeed, in this case, $\gamma_1 > 0$ and $\gamma_2 > 0$ must hold. When $\gamma_1 > 0$ and $\gamma_2 > 0$, solving the Kuhn-Tucker conditions, we obtain $\gamma_1^* = \frac{b_1 + c_1}{x_1}$, $p_1^* = \frac{b_1 - c_1}{2}$, $\gamma_2^* = \frac{b_2 + c_2}{x_2}$ and $p_2^* = \frac{b_2 - c_2}{2}$. (4) If $x_1 = 0$ and $x_2 = 0$, then the platform will not make any trading decisions either.

## A.2 Proof of Proposition 2

**Proof.** The first order conditions are

$$\frac{\partial u_i}{\partial x_1} = (\alpha - s)[1 - F(\underline{v})] - x_1 \leq 0, x_1 \geq 0 \tag{34}$$

$$\frac{\partial u_i}{\partial x_2} = m - \phi x_2 \leq 0, x_2 \geq 0 \tag{35}$$

If $x_1 = 0$, then inequality (34) implies $\alpha < s$, must be the case. If $x_1 > 0$, then the equation (34) holds with strict equality implying $x_1^* = (\alpha - s)[1 - F(\underline{v})]$,

where $\alpha > s$ must be the case.

If $x_2 = 0$, then inequality (35) leads to $m \leq 0$. Since $m > 0$, $x_2 = 0$ is impossible. If $x_2 > 0$, then solving $\frac{\partial u_i}{\partial x_2} = 0$ can derive $x_2^* = \frac{\phi}{m}$. Note that the second-order conditions are satisfied in these cases.

## A.3 Proof of Proposition 3

**Proof.**

$$\frac{\partial \pi_P^*}{\partial c_1} = b_1 + c_1 - (\alpha - s)[1 - F(\underline{v})] \leq 0 \tag{36}$$

using equation (22). I.e. higher values of $c_1$ lower profit $\pi_P^*$ given (equilibrium) values of $\gamma_1^*$. Similarly,

$$\frac{\partial \pi_P^*}{\partial c_2} = b_2 + c_2 - \frac{m}{\phi} \leq 0 \tag{37}$$

I.e. as $c_2$ becomes higher, profits $\pi_P^*$ will be lowered given (equilibrium) values of $\gamma_2^*$.

## A.4 Proof of Proposition 4

**Proof.** $\frac{\partial \gamma_2^*}{\partial \phi} = \frac{b_2 + c}{m} > 0$. *Therefore, when $\phi$ becomes higher, $\gamma_2^*$ will also become higher.* $\frac{\partial \pi_P^*}{\partial \phi} = \frac{m}{\phi^2} > 0$. *Therefore, when $\phi$ becomes higher, $\pi_P^*$ will also become higher.*

# References


[1] Acemoglu, D., Makhdoumi, A., Malekian, A. and Ozdaglar, A., 2022. Too much data: Prices and inefficiencies in data markets. American Economic Journal: Microeconomics, 14(4), pp.218-256.

[2] Acquisti, A., Taylor, C. and Wagman, L., 2016. The economics of privacy.*Journal of economic Literature*, 54(2), pp.442-92.

[3] Bataineh, A.S., Mizouni, R., Bentahar, J. and El Barachi, M., 2020. Toward monetizing personal data: A two-sided market analysis. Future Generation Computer Systems, 111, pp.435-459.

[4] Choi, J.P., Jeon, D.S. and Kim, B.C., 2019. Privacy and personal data collection with information externalities. Journal of Public Economics, 173, pp.113-124.

[5] Dimakopoulos, P.D. and Sudaric, S., 2018. Privacy and platform competition. International Journal of Industrial Organization, 61, pp.686-713.

[6] Duan, Y., Liu, P. and Feng, Y., 2022. Pricing strategies of two-sided platforms considering privacy concerns. *Journal of Retailing and Consumer Services*, 64, p.102781.

[7] Goldfarb, A. and Que, V.F., 2023. The Economics of Digital Privacy. Annual Review of Economics, 15.

[8] Fainmesser, I.P., Galeotti, A. and Momot, R., 2023. Digital privacy. Management Science, 69(6), pp.3157-3173.

[9] Frik, A. and Mittone, L., 2019. Factors influencing the perception of website privacy trustworthiness and users' purchasing intentions: The behavioral economics perspective. Journal of theoretical and applied electronic commerce research, 14(3), pp.89-125.

[10] Goldfarb, A. and Tucker, C., 2012. Shifts in privacy concerns. American Economic Review, 102(3), pp.349-53.

[11] Hann, I.H., Hui, K.L., Lee, S.Y.T. and Png, I.P., 2007. Overcoming online information privacy concerns: An information-processing theory approach. Journal of management information systems, 24(2), pp.13-42

[12] Ichihashi, S., 2020. Online privacy and information disclosure by consumers. American Economic Review, 110(2), pp.569-595.

[13] Ichihashi, S., 2023. Dynamic privacy choices. American Economic Journal: Microeconomics, 15(2), pp.1-40.

[14] Lam, W.M.W. and Seifert, J., 2023. Regulating data privacy and cybersecurity. The Journal of Industrial Economics.

[15] Lee, D.J., Ahn, J.H. and Bang, Y., 2011. Managing consumer privacy concerns in personalization: a strategic analysis of privacy protection. Mis Quarterly, pp.423-444.

[16] Lutz, C., Hoffmann, C.P., Bucher, E. and Fieseler, C., 2018. The role of privacy concerns in the sharing economy. Information, Communication and Society, 21(10), pp.1472-1492.

[17] Madden, M., 2012. Privacy management on social media sites. *Pew Internet Report*, 24, pp.1-20.

[18] Martin, K., 2018. The penalty for privacy violations: How privacy violations impact trust online. Journal of Business Research, 82, pp.103-116.

[19] Norberg, P.A., Horne, D.R. and Horne, D.A., 2007. The privacy paradox: Personal information disclosure intentions versus behaviors. Journal of consumer affairs, 41(1), pp.100-126.

[20] Pallant, J.I., Pallant, J.L., Sands, S.J., Ferraro, C.R. and Afifi, E., 2022. When and how consumers are willing to exchange data with retailers: An exploratory segmentation. Journal of Retailing and Consumer Services, 64, p.102774.

[21] Ray, S., Palanivel, T., Herman, N. and Li, Y., 2021. Dynamics in Data Privacy and Sharing Economics. IEEE Transactions on Technology and Society.

[22] Taylor, C. and Wagman, L., 2014. Consumer privacy in oligopolistic markets: Winners, losers, and welfare. *International Journal of Industrial Organization*, 34, pp.80-84.