ICIS 2023 Proceedings

International Conference on Information Systems (ICIS)

December 2023

The Economic Implications of Privacy Dark Patterns (PDPs)

Dawei Chen
National University of Singapore, dawei@comp.nus.edu.sg

Jungpil Hahn
National University of Singapore, jungpil@nus.edu.sg

The Economic Implications of Privacy Dark Patterns (PDPs)

Completed Research Paper

Dawei Chen
National University of Singapore
11 Research Link, Singapore 119391
dawei@u.nus.edu

Jungpil Hahn
National University of Singapore
11 Research Link, Singapore 119391
jungpil@nus.edu.sg

Abstract

This study investigates the economic implications of privacy dark patterns (PDPs) through which firms "wisely" play privacy games. It is believed that PDPs advantage firms by deceiving consumers. However, it could also hinder firms' credibility. Thus, we aim to examine whether PDPs always benefit firms and hurt consumers. We also seek to answer whether market forces are sufficient to keep PDPs at relatively low levels. Our results show that PDPs make users weakly worse off and the seller weakly better off. Nevertheless, the seller has incentives to not utilize any PDPs when users' privacy cost is high, and the ratio of privacy concern and search cost is either too high or too low under which market shrinkage effect dominates market division effect. Finally, we show that a welfare maximizing social planner would allow the presence of PDPs when users' privacy cost is sufficiently low.

Keywords: Privacy, privacy dark patterns, analytical modeling, users information disclosure

Introduction

Consumers are empowered with sophisticated privacy rights in the era of privacy. For instance, Chapter 3 of the General Data Protection Regulation 2016 (GDPR) states that data subjects have the rights to *information*, *access*, *rectification*, *erasure*, *restriction*, *data portability* and *object* regarding their personal information.[1] In reality, the exercise of these privacy rights depends on the technical infrastructures provided by data collectors. For example, when consumers visit a website which collects their personal information through cookies, they will be asked to make consent choices with respect to personal information provision among several options, but these options are carefully designed by the website (i.e., by the data collectors). Due to the substantial value of consumer personal information, data collectors (i.e., the websites) have a strong incentive to carefully engineer the privacy infrastructures (i.e, the consent interfaces) such that they can collect as much personal information from the data subjects (i.e., consumers), which gives rise to the proliferation of privacy dark pattern (PDP) practices.

Privacy dark pattern (PDP) refers to "building blocks that are used by service providers to deceive and mislead their users" (Bösch et al. 2016, pp. 243). They are intentionally utilized by data collectors to enrich the collection of personal information from their users. Ironically, despite increasing privacy regulation, PDP practices are becoming more ubiquitous in a variety of contexts. Nouwens et al. (2020) showed that around 90% of surveyed websites in the UK which contain consent management features adopt some forms of PDP practices. These PDP practices include implicit consent, making rejecting all tracking cookies more difficult than accepting all cookies, and pre-ticked checkboxes, among others. Similarly, the European Data Protection Board (EDPB) identified a list of PDP practices in the context of social media platforms, namely, *overloading*, *skipping*, *stirring*, *hindering*, *confusing*, and *hiding* (EDPB 2022).

[1] GDPR 2016, Chapter 3: https://gdpr-info.eu/chapter-3/

The focus of the early literature on privacy dark pattern has been to understand its descriptive aspects, namely, to define and classify privacy dark pattern via taxonomies (Bösch et al. 2016; Mathur et al. 2021). Subsequently, the literature establish the prevalence of PDP practices in different contexts, such as on consent management platforms (Nouwens et al. 2020), online shopping websites (Mathur et al. 2019), and mobile apps (Di Geronimo et al. 2020). Researchers investigate the effectiveness of PDP practices either from a descriptive paradigm (Frobrukerr$\mathring{a}$det 2018; Mathur et al. 2021) or using online survey-based experiments (Luguri and Strahilevitz 2021; Nouwens et al. 2020). There is, however, a lack of normative work to quantify the economic implications of privacy dark pattern practices.

Theoretical understanding of the economic implications of PDP practices is still quite nascent. The majority of prior works argued simplistically that PDP practices could benefit data collectors (i.e., websites, platforms, apps developers, etc.) while harm data subjects since they go against data subjects' "best interest" and empower data collectors to collect a greater amount of personal information. This argument, however, depends on the assumption that users are fully deceived by the PDP practices. However, in reality, some users can recognize the presence of PDP practices and may retaliate. In addition, if the PDP practice is too egregious, it can lead to repercussions and hurt the data collectors' credibility (Luguri and Strahilevitz 2021). As such, the optimal level of PDP practices for the data collector depends on the relative magnitude of the benefit derived from deception (e.g., collecting more personal information which can lead to greater ability to price discriminate) and the cost incurred when PDP is recognized by data subjects (e.g., loss of personal information which can lead to lost sales opportunities). In particular, it depends on the level of sophistication of data subjects (i.e., whether they can identify the presence of PDPs) and their sensitivity to PDP (i.e., how they will respond when recognizing the presence of PDP). Therefore, the first research question this study seeks to answer is: *Do privacy dark pattern (PDP) practices always benefit the data collector and hurt data subjects?*

This study also tries to examine whether additional and what kinds of regulation rules are needed to protect data subjects from PDP practices. Given the deceptive nature of PDP, regulators can clearly assert what constitutes dark patterns and can fully ban their use. For instance, the Commission Nationale de L'Informatique et des Libertés (CNIL) in France shed light on the necessary control of design and architecture of privacy choices (CNIL 2019). Recently, the US Federal Trade Commission (FTC) held a workshop to discuss how dark patterns affect consumers and the marketplace, and further called for comments on regulation over dark patterns (FTC 2021). In addition, the European Data Protection Board (EDPB) provided guidelines on dark patterns for social media platform interfaces (EDPB 2022). The newly proposed California's Privacy Rights Act (CPRA) also clearly stated that "any agreement obtained through the use of dark patterns shall not constitute consumer consent" (CCPA 2022). Therefore, we investigate *whether market forces are sufficient to keep PDP practices at low levels* and *what is the optimal regulation on PDP practices*.

In this paper, we develop a game-theory model of privacy dark pattern (PDP). In the benchmark setup, a monopoly seller offers a single product to many users. The seller chooses the level of PDP practices to influence users' information disclosure behavior. After observing the information provided by users, the seller decides the pricing strategy which in turn determines users' purchase decision. Our results show that the presence of PDP practices indeed make users weakly worse off and the seller weakly better off. Nevertheless, the seller has incentives to not utilize any PDP practices when users' privacy cost is high and the ratio of privacy concern and the reduced search cost of opting-in is either too high or too low. This could be attributed to the fact that the *market shrinkage effect* dominates the *market division effect* under these conditions. In other words, the gain from making more users opt-in will be outweighed by the loss from total market shrinking when the seller increases the PDP level. Finally, we show that a welfare maximizing social planner would allow the presence of PDP when the users' privacy cost is low enough.

To the best of our knowledge, our paper is the first to examine the economic implications of privacy dark pattern. This study extends the existing literature on dark patterns by normatively investigating the conditions under which a seller will employ PDP. We also offer implications to policy makers on how to regulate the proliferation of PDP.

The reminder of the paper is organized as follows. A literature review is first provided. We then present the benchmark model, a model with only naïve users and, finally, a model with sophisticated users. Subsequent sections present discussions on the impact of PDP, static comparative analysis and implications for regulation. We conclude with a discussion of findings, limitations and future work.

Related Literature

The main purpose of our study is to examine the economic implications of privacy dark pattern. Firstly, privacy dark pattern is one type of dark patterns. Secondly, it influences consumers' privacy protection behaviors. Thirdly, a seller will utilize disclosed personal information to learn consumers' preferences and further conduct price discrimination. Therefore, our work is related to three streams of literature: (i) dark patterns, (ii) privacy protection, and (iii) price discrimination.

Dark Patterns

The stream of literature that is closest to our work is the one on dark patterns. Prior work has primarily been descriptive and attempted to clearly define dark patterns and develop conceptual taxonomies of dark patterns. Only a few studies which investigate the prevalence and effectiveness of dark patterns have been normative. In this section, following a chronological order, we briefly review three waves of the literature on dark patterns.

The first wave of dark patterns research consists of works which seek to provide a definition and a taxonomy for better understanding dark patterns. In 2010, the term "dark pattern" first appeared on Harry Brignull's website *darkpattern.org* [2] where he provided a list of 12 types of deceptive designs widely used on websites and apps. Inspired by Brignull's work, follow-up research shed light on a more specific definition and taxonomy of dark patterns in different contexts. For instance, Mathur et al. (2019) found 15 types dark patterns within 7 broader categories, namely, *sneaking*, *urgency*, *misdirection*, *social proof*, *scarcity*, *obstruction*, and *forced action*, in online shopping websites. In the online privacy context, Bösch et al. (2016) revealed 7 types of privacy dark patterns: *privacy zuckering*, *bad defaults*, *forced registration*, *hidden legalese stipulations*, *immortal accounts*, *address book leeching*, and *shadow user profiles*. Recently, Mathur et al. (2021) conducted a comprehensive review of prior work and took a step beyond mere definition and classification. They proposed six high-level attributes (*asymmetry*, *restrictiveness*, *disparate treatment*, *covertness*, *deception*, and *information hiding*) to organize different instances of dark patterns in prior work. In addition, they further grouped these attributes into two themes – "modifying the decision space" and "manipulation the information flow."

The second wave of research examines the pervasiveness of dark patterns. Mathur et al. (2019) revealed that more than 11% of online shopping websites in the UK contain dark patterns. In addition, the presence of dark patterns is identified on more than 95% of free Android apps in the US Google Play Store (Di Geronimo et al. 2020). In consent management platform interface design, (Nouwens et al. 2020) found that only 11.8% websites they surveyed do not use any dark pattern designs. Di Geronimo et al. (2020) reported that 95% of the popular mobile apps they analyzed employed at least one type of dark patterns. The growing prevalence of dark patterns has attracted researchers' attention to investigate their effectiveness and impact on various stakeholders (i.e., consumers, websites, third-parties, etc.).

The third wave of the literature on dark patterns investigates their effectiveness and consequences. The majority of the literature from a HCI research perspective concluded that most of the dark patterns interfaces designs can effectively deceive and persuade consumers to take actions that go against their best interests but benefit the designers (i.e., website operators, app developers, platform operators, etc.) (Di Geronimo et al. 2020; Luguri and Strahilevitz 2021; Nouwens et al. 2020). In two online experiments, Luguri and Strahilevitz (2021) showed that increasing the "dark" level of interface design could raise users' subscription rates for a paid data protection program. In their work which examined the impact of notification style (i.e., barrier vs. banner) and bulk consent buttons (i.e., accept all and/or reject all) on users' cookies consent responses, Nouwens et al. (2020, pp. 8-9) found that "removing the 'reject all' button from the first page increased the probability of consent by 22-23 percentage points" and "displaying more granular consent choices on the first page decreased the probability of consent by 8-20 percentage points." The effectiveness

[2] Brignull's deceptive design website: https://www.deceptive.design/

of dark patterns is often attributed to the limits of human rationality and cognitive capabilities. Bösch et al. (2016) argued that, due to the fact that users either have no motivation or no opportunity to effortfully think and reason when they make privacy decisions since they typically lack the required knowledge, ability, or time, individuals often make privacy decisions quickly, intuitively, unconsciously, and automatically.

Conversely, other scholars have shed light on the negative consequences of dark patterns for designers. Luguri and Strahilevitz (2021) revealed that respondents who are exposed to aggressive dark pattern conditions and make a decline decision reported more negative emotions. Studies have also showed that native ads, one type of dark patterns, contribute to lower trustworthiness for the websites (Aribarg and Schwartz 2020). Short-term benefit might be gained through using dark patterns to deceive new customers, however, practitioners argue that they will fail in the long run since loyal consumers who are more valuable than new customers will realize the deception and terminate the relationship (Brownlee 2016).

The work that is perhaps closet to our study is Wu et al. (2022). They studied one type of dark patterns, namely, *native ads*. They argue that increasing the opaqueness of native ads can increase the click-through rate but will reduce the number of website visitors since inattentive consumers will be more dissatisfied and form the belief that the publisher's quality is low. Therefore, due to its signaling role, in equilibrium, the opaqueness of native ads is low in order to signal their high quality. However, strict regulations will eliminate this self-regulated market force and yield lower consumer surplus and social welfare. In our paper, we focus on another type of dark pattern: the privacy dark pattern.

To the best of our knowledge, our paper is the first to examine the economic implications of privacy dark patterns beyond mere description (i.e., definition and classification) from prior work. We build a game-theoretic model to explore under which conditions it is optimal for a digital business to employ privacy dark patterns and what kind of regulation over privacy dark patterns might need to be introduced in order to maximize social welfare.

Privacy Protection

The economics of privacy has been extensively documented in the literature. Acquisti et al. (2016) provides a comprehensive review. In this section, we briefly summarize those recent and most relevant works. In essence, consumers can decide how much personal information to disclose as consumers are empowered with increasing control over their personal information in the era of privacy. As the consequences of privacy protection vary greatly with context, such as the consumer's decision space, how firms exploit consumer information and for what purposes (Acquisti et al. 2016), we discuss below some of the more closely related recent works.

Koh et al. (2017) consider a model of a monopolistic seller who chooses two separate prices, whereas consumers decide whether to opt-in or opt-out and whether to buy the seller's product after observing the price. Consumers face a trade-off between personalized price, privacy cost and reduced search cost when they decide whether to opt-in or opt-out. They show that empowering consumers with binary privacy choices does not necessarily increase consumer surplus nor social welfare. Rather, it depends on the intrinsic costs of privacy and whether or not personalized pricing is possible.

Dengler and Prüfer (2021) examine the impact of consumers' strategic sophistication level in a setting similar to Koh et al. (2017) but while assuming that the seller can perfectly infer consumers' types. They show that unlimited consumer sophistication results in the existence of anonymization behaviors even without the presence of privacy costs. In addition, increasing consumer sophistication will make consumers worse off while the seller's profits and overall social welfare will increase. These results rely on the assumption that a monopolist can conduct perfect price discrimination for "opt-in" consumers and consumers will choose "opt-in" when they are indifferent between "opt-in" and "opt-out".

Ichihashi (2020) investigates consumers' information disclosure behavior and a multi-products monopolist's pricing strategy. Consumers face the trade-off between accurate recommendations and price discrimination when they disclose personal information. In a restricted model, consumers can tell the seller which is their favorite product and the seller will always have the incentive to recommend this product to the consumers. He shows that, counter-intuitively, the seller "prefers to commit to not use information for pricing in order to encourage information disclsoure" (Ichihashi 2020, pp. 569) as the demand effect will dominate the price discrimination effect.

Different from the above binary and special consumers privacy choices context, Ali et al. (2023) study the welfare implications of general consumer privacy choices. In their model, a consumer with valuation $v \in [0, 1]$ can send a message of the form "my type is in the set $[a, b]$" to the seller. They find that simple evidence (i.e., binary privacy choice) does not help consumers while rich evidence could lead to a Pareto-improving equilibrium. Thus, they conclude that consumers' control over data benefits them when they can choose not only *whether* to communicate but also *what* to communicate.

Choi et al. (2020) examine the implications of the binary consumer privacy choice (opt-in vs. opt-out) on a platform's ad pricing and two firms' product pricing strategies. Consumers face a trade-off between the cost from price discrimination and the benefit from intensifying product price competition when they choose to opt-in. They show that empowering consumers' privacy choice can weakly increase consumer surplus and decrease firms' profit. The impact on the ad platform's profit depends on the accuracy of the signal from the opt-in consumers and the extent of product differentiation.

Different from the above works which focus on one-period consumers' privacy choice, Ichihashi (2023) considers a dynamic infinite game where a consumer chooses an activity level in each period which signals his type and the platform decides the privacy protection level either under long-run or short-run commitment. He shows that, under the long-run commitment regime, the platform can commit to gradually decrease the privacy protection level but the consumer will choose high activity levels even though he loses privacy and receives low payoffs since the consumer expects high privacy protection or has already lost his privacy in the long run. Nevertheless, when the platform cannot commit to future privacy protection, it may fail to collect any information.

Using a queuing model, Hu et al. (2022) examine the interaction between strategic consumers who are empowered with a binary privacy choice (i.e., disclose or withhold their personal information) and a service provider who implements a preemptive priority queue policy. Their results reveal that giving consumers control over their privacy could actually hurt them when the service provider operates under the shortest processing time first (SPT) policy.

To the best of our knowledge, our work is the first one to examine the economic implications of PDP. We investigate the firm's incentive to deploy deceptive interface designs to affect consumers' information disclosure behaviors which further influences the firm's pricing strategy and consumers' purchasing behaviors.

Privacy and Price Discrimination

Privacy protection and price discrimination are two sides of the same coin. However, the traditional price discrimination literature has not explicitly considered privacy issues. Advances in information tracking, collection and mining technologies have enabled digital businesses to achieve first degree price discrimination (Acquisti et al. 2016). Nevertheless, the introduction of privacy protection could restrict the collection of certain sensitive information (e.g., biometric information) or even generate new "information" which can significantly affect a digital business's price discrimination strategies.

The literature has documented that privacy protection impedes and reshapes a digital business's price discrimination ability and strategy (Ali et al. 2023; Dengler and Prüfer 2021; Ichihashi 2020; Koh et al. 2017). The impact highly depends on how and what users personal information is protected (i.e., no vs. full protection (Choi et al. 2020; Dengler and Prüfer 2021; Hu et al. 2022; Koh et al. 2017), arbitrary protection (Ali et al. 2023)), the signal structure from privacy protection (Armstrong and Zhou 2022), how the digital business utilizes the collected information (i.e., whether the digital business is allowed to (Koh et al. 2017) or commit to (Ichihashi 2020) perform personalized pricing) and market competition (Ali et al. 2023). Our work moves beyond this research paradigm to investigate how PDPs influence the impact of consumers' privacy protection and the digital business following a price discrimination strategy.

Model Setup

Before we step into the specific model setting, a motivating example is provided to toward a better understanding of the model setup. Imagine that there is a online store owner (i.e., the seller) who decides the information collection practices on his website. Since individuals are empowered with the right of consent by privacy law, the online store owner is required to design a proper cookies consent interface. Whenever a user (i.e., the consumer) visits this website, it asks her for cookies consent (i.e., opt-in or opt-out) (how much information you would like to disclose to the website). If the user chooses to opt-in, the website will learn her preference via data analytics which empowers the website to conduct price discrimination and offers a personalised price to the visitor. If the user chooses to opt-out (i.e., no information disclosure), the website cannot learn the user's preference and can only offer her a uniform price. Finally, given the offered price, the user decides whether or not to purchase the product.

Briefly, the seller will decide the privacy dark pattern level (i.e., cookies consent interface) on his website, a personalised price for opt-in users and a uniform price for opt-out users. The users make their information disclosure (i.e., opt-in or opt-out) and purchase (i.e., buy or not buy) decisions. In the following section, we will illustrate our players' (the seller, user) behavior with respect to their decision variables, utility function and information structure.

Our model consists of a monopolistic seller who sells a single product to a mass of users who purchase at most one unit of the product. Transactions between users are not allowed. The marginal production cost is constant and normalized to zero. Users have heterogeneous valuation v over the product, where, without loss of generality, $v \sim \mathcal{U}[0, 1]$.

Seller Behavior

Privacy Dark Patterns

The seller decides how to project the privacy-related interfaces (e.g., cookies consent pop-up). We abstract away from the details of how privacy dark patterns might be embedded into the privacy-related interfaces, such as which attribute and category of privacy dark patterns (Mathur et al. 2021) are utilized. In our model, the seller simply chooses the level of privacy dark pattern (PDP) $d \in [0, 1]$, which indicates how difficult it is for users to opt-out. In practice, the seller can control d by hiding the opt-out option behind several pages, by making opt-in as default option, or by obscuring the presentation of necessary information.

The PDP level d influences users' information disclosure and purchase behavior in two ways. On the one hand, we operationalize the PDP level d such that there is an additional cost d when users choose to opt-out in order to capture the feature that PDP makes opt-out more difficult to choose such that users are more likely to disclose information (i.e., choose to "accept all" or opt-in). On the other hand, a λd proportion of users will directly choose to opt-out and not buy the product regardless of the future price(s) when users are sophisticated in order to capture the idea that the PDP practices may hurt firms' credibility (Wu et al. 2022) and some users may react negatively over it (Aribarg and Schwartz 2020; Brownlee 2016; Luguri and Strahilevitz 2021)[3].

Pricing Regimes

In our model, the seller has the ability to observe and differentiate opt-in and opt-out users so that he can set different prices for opt-in and opt-out users. He can collect personal information from those opt-in users which empowers user preference learning. Whereas, the seller cannot learn opt-out users' preferences without information disclosure. Therefore, the seller can set a personalized price $P_{in}(\hat{v})$ for the opt-in users based on what he has learned from the personal information disclosed by the opt-in users and a uniform price P_{out} for the opt-out users.

[3] We thank one of the anonymous reviewers for pointing out an alternative way to model this credibility loss by introducing d into opt-in users' utility function. We will explore this alternative model specification in future research

Seller's Profit

In essence, the seller is rational and profit maximizing by choosing an optimal PDP level d, a personalised price $P_{in}(\hat{v})$ for a opt-in user with valuation v and a uniform price P_{out} for opt-out users. The seller's profit function is:

$$\pi\left(P_{in}(\hat{v}),\ P_{out},\ d\right) = P_{in}(\hat{v}) \times D_{in}(P_{in}(\hat{v}),\ P_{out},\ d) + P_{out} \times D_{out}(P_{in}(\hat{v}),\ P_{out},\ d) \tag{1}$$

Users Behaviour

Information Disclosure

Users Decision Space – Users face two choices, opt-in or opt-out, when they decide whether or not to disclose their personal information. The literature has modeled users' decision space over information disclosure or privacy protection in different ways. The most prevalent decision space is binary choices, such as no vs. full disclosure, and opt-in vs. opt-out (Choi et al. 2020; Dengler and Prüfer 2021; Hu et al. 2022; Koh et al. 2017) [4]. Since our main purpose is to examine the economic implications of PDP and most privacy-related interface designs (i.e., cookies consent pop-up) only allow users to make discrete choices (typically "accept all" or "reject all"), we formulate users' information disclosure choice as either to opt-in or to opt-out.

Signal Structure – The signal structure conceptualizes how much the seller can learn from opt-in users' information disclosure. Mathematically, it is a mapping from users' true valuation v to the signal realization $\hat{v}$ observed by the seller. The literature has documented different types of signal structures (Armstrong and Zhou 2022). To simplify our presentation and obtain closed-form solutions, we assume that when a user chooses to opt-in, the seller can perfectly predict her valuation (i.e., $\hat{v} = v$) (Dengler and Prüfer 2021).

Cost: Privacy Concern – Apart from heterogeneity in product valuation, users are also heterogeneous in privacy concern with respect to information disclosure. Users will incur privacy costs when they choose to disclose personal information. These costs could be instrumental or intrinsic (Lin 2022). Instrumental privacy costs consist of price discrimination (Ali et al. 2023), potential data breach (Goode et al. 2017), marketing solicitations (Hann et al. 2008), etc. Intrinsic privacy costs relate to the loss of autonomy, invasion of privacy rights (Chellappa and Shivendu 2007), etc. In our model, a proportion $\alpha \in [0, 1]$ of users are privacy sensitive (labeled as *S* users) and they will encounter a positive intrinsic privacy cost $r \in [0, 1]$, whereas the remaining $1 - \alpha$ users are privacy non-sensitive (labeled as *NS* users) whose intrinsic privacy cost is normalized to zero.

Benefit: Personalization – Apart from the cost (here, price discrimination and privacy concern), the benefit of information disclosure has also been extensively documented in the literature (Acquisti et al. 2016; Hidir and Vellodi 2021; Ichihashi 2020; Koh et al. 2017). For example, Koh et al. (2017) model the benefit of disclosing personal information as reduction in search costs when users decide to purchase the product. Ichihashi (2020) models the benefit of information provision as an increase in the relevance of recommended product. In our model, for simplicity, we assume that there is a constant search cost $c \in [0, 1]$ for opt-out users when they choose to buy the product since it takes effort for them to collect, review and analyze product information. Conversely, with the help of information disclosure and personalization, the search cost for opt-in users is normalized to zero. For both opt-in and opt-out users, it does not incur any search cost if they do not buy the product.

Users' Utility

Taken together, the users' utility consists of product valuation v, product price $P_{in}(v)$ or P_{out}, privacy cost r, search cost c and additional cost d imposed by privacy dark patterns. The utilities of *S* and *NS* type users are presented in Table 1, where $r = 0$ for privacy non-sensitive (*NS*) users and $r > 0$ for privacy sensitive (*S*) users. The value of the outside option of not-purchasing is normalized to zero.

[4] Apart from this common practice, Ali et al. (2023) assume that consumers can send a message of the form "my type is in the set $[a, b]$" to the seller; Ichihashi (2020) formulates the consumer's privacy choice as a Blackwell experiment about his valuation over multiple products.

Additional Assumptions

Assumption 1: Users choose to "Opt-in " when they are indifferent between "Opt-in" and "Opt-out." Since the seller has the ability to perfectly infer those opt-in users' valuation and conduct first degree price discrimination, when a user is indifferent between opt-in and opt-out, the seller has the incentive and ability to set a lightly lower $P_{in}(v)$ (i.e., by a small positive number ϵ) such that this user will choose to opt-in ($U_{in} > U_{out}$). Taking the limitation with respect to ϵ is equivalent to the simplified assumption that users choose to opt-in when they are indifferent between opt-in and opt-out.

	Buy	Not-Buy
Opt-In	$v - P_{in} - r$	$-r$
Opt-Out	$v - P_{out} - c - d$	$-d$

Table 1. Utility of a User with Valuation v

Assumption 2: Users choose to "Buy" when they are indifferent between "Buy" or "Not-buy." For opt-in users, similarly, when they are indifferent between "Buy" and "Not-buy", the seller can charge a slightly lower price P_{in} such that they will choose to "Buy" rather than "Not-buy." It is simply equivalent to assume that they choose to "Buy" when they are indifferent between "Buy" and "Not-buy." For opt-out users, since the price P_{out} is uniform, there is only one marginal user. Mathematically, a single point will not affect the integration results. Taken together, for simplification, we assume that users choose to "Buy" when they are indifferent between "Buy" and "Not-buy".

Game Sequence and Solution Concept

Timing of the Game – The sequence of the game is presented in Figure 1. In stage 1, the seller chooses the level of privacy dark pattern (PDP) practices d. After observing the PDP level, users make their information disclosure decision using the expected prices (i.e., $E[P_{in}(v)]$ and $E[P_{out}]$) in stage 2. In stage 3, after observing the signal realizations and updating his belief on opt-out users' valuation, the seller determines the personalized price $P_{in}(v)$ for opt-in users and a uniform price P_{out} for opt-out users. Finally, in stage 4, after observing the offered prices, both opt-in and opt-out users make purchase decisions and all payoffs are realized.

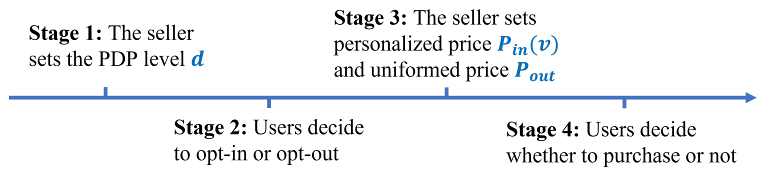

Stage 1: The seller sets the PDP level d
Stage 3: The seller sets personalized price $P_{in}(v)$ and uniformed price P_{out}
Stage 2: Users decide to opt-in or opt-out
Stage 4: Users decide whether to purchase or not

Figure 1. Sequence of the Game

Solution Concept – Since the seller can perfectly predict opt-in users' product valuation, he will have the knowledge of the valuation distribution among opt-in users and opt-out users. All other information is common knowledge. The seller and users are fully rational such that $E[P_{in}(v)] = P_{in}(v)$ and $E[P_{out}] = P_{out}$). Thus, we have a sequential game with complete information and consequently we use the sub-game perfect equilibrium (SPB) as our solution concept. A summary of the notation is provided in Table 2.

Model Analysis

Benchmark Case: No PDP

We use the no privacy dark pattern (PDP) case as our benchmark and denote it using superscript b. The sequence of the game under no PDP is the same as the one depicted in Figure 1 without stage 1 where the seller sets the PDP level d. We use the backward induction approach to derive the equilibrium.

Notations	Descriptions
α	Proportion of privacy sensitive users; $\alpha \in [0, 1]$
v	Users' product valuation; $v \sim \mathcal{U}[0, 1]$
$\hat{v}$	User's valuation observed by the seller; $\hat{v} = v$
r	Intrinsic privacy cost; $r \in [0, 1]$
c	Search cost when opt-out users decide to buy; $c \in [0, 1]$
λ	Privacy dark pattern sensitivity; $\lambda \in R^+$
d	Level of privacy dark pattern; $d \in R^+$
P_{in}	Price for opt-in users; $P_{in} \in R^+$
P_{out}	Price for opt-out users; $P_{out} \in R^+$
π	Seller's profit
CS	Users surplus
TW	Total social welfare
superscript b	Denote benchmark solution
superscript n	Denote naïve users model solution
superscript s	Denote sophisticated users model solution
superscript w	Denote social welfare maximizing solution

Table 2. Summary of Notation

Stage 4: Buying – According to the utilities (see Table 1), opt-in users will buy the product if the personalised price $P_{in}(v)$ does not exceed their valuation since the privacy cost r is a sunk cost (as long as a user chooses to opt-in, there will be a privacy cost r regardless of her subsequent purchase decision). On the contrary, search cost c is only incurred when a opt-out user decides to purchase the product. Thus, opt-out users whose valuation is greater than $P_{out} + c$ will buy the product.

Stage 3: Pricing $P_{in}(v)$ and P_{out} – Knowing v precisely for all opt-in users, the seller will sets the following personalized price for opt-in users:

$$P_{in}^{b^*}(v) = v \tag{2}$$

Firstly, the seller has no incentive to set a personalized price $P_{in}(v)$ lower than the true valuation v it observes from an opt-in user v since he can gain higher revenue through slightly increasing $P_{in}(v)$ (i.e., by a small positive number ϵ) to extract more surplus while the user v still decides to opt-in and buy the product. In addition, the seller has no commitment power to commit a lower $P_{in}(v)$ in order to persuade users to disclose more information (i.e., choose to opt-in rather than opt-out) in stage 2. Secondly, the seller also has no incentive to set a higher $P_{in}(v)$ (i.e., greater than v), otherwise, he will lose all opt-in users. Therefore, the seller will set a personalized price equal to the true valuations for each opt-in user and all opt-in users will buy the product (see additional assumption 2).

Since the seller is uninformed about opt-out users' valuation distribution, he cannot derive the demand from opt-out users given a uniform price P_{out} which makes it impossible to find out the optimal price P_{out} for opt-out users at this moment. However, the seller can infer opt-out users' valuation distribution according to how users react to the above expected pricing strategy for opt-in users. Thus, let us firstly analyze users' information disclosure behavior (opt-in vs. opt-out) in stage 2.

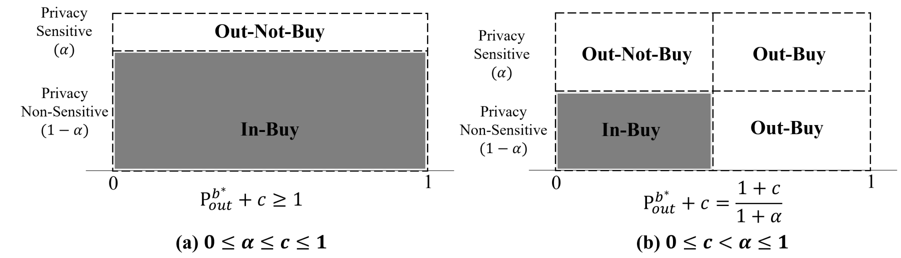
Stage 2: Opt-in/Opt-out – When making the information disclosure decision, fully rational users will completely anticipate the above pricing strategy for opt-in users. Thus, privacy sensitive users will know that they will receive a utility of $-r$ if they choose to opt-in, while privacy non-sensitive users will expect a utility of 0 if they choose to opt-in. In addition, they will form an expected price $E(P_{out})$ for opt-out. Since both the seller and the users are fully rational, the expected price $E(P_{out})$ should be equal to the real price P_{out} in equilibrium. For simplification, we directly use the notation P_{out} in the following analysis. Therefore, given the expected $P_{in}(v)$ and P_{out}, when choosing to opt-in or opt out, users maximize their utilities in Table 1. As can be seen, privacy sensitive (*S*) users will **never** choose to opt-in since they can gain a higher utility by choosing to opt-out (at least 0).

Stage 3: Pricing $P_{in}(v)$ and P_{out}(revisited) – Given how users will form expectation on $P_{in}(v)$ and P_{out}, and how they will respond to these expected prices, the seller maximizes its profit given by equation (1) with respect to P_{out}. This yields the optimal price P_{out} for opt-out users when there PDP is not at play:

$$P_{out}^{b^*} = \begin{cases} \dfrac{1-\alpha c}{1+\alpha}, & 0 \leq c < \alpha \leq 1 \\ \underline{P_{out}}, & 0 \leq \alpha \leq c \leq 1, \; where \; \underline{P_{out}} \geq 1-c \end{cases} \tag{3}$$

As can be seen, when the proportion of privacy sensitive users (α) is smaller than the reduced search cost (c) through opt-in; in other words, when the benefit of opt-in is high (i.e., high c) and users are less concerned about their privacy (i.e., low α), the profit-maximizing seller would only cover the opt-in users market by setting a high price P_{out} for opt-out users. This could be attributed to the fact that, when users are less concerned about privacy, increasing P_{out} will dramatically expand the market size of opt-in users while slightly reduce the market size of opt-out users. Thus, the profit gained from the opt-in users market will surpass the loss from the shrinkage of the opt-out users market. On the contrary, the seller prefers to set a moderate P_{out} for opt-out users when the proportion of privacy sensitive users (α) is larger which reflects current trends in the era of privacy.

Taken together, the users segmentation of the benchmark equilibrium is depicted in Figure 2. In the equilibrium under high α (Figure 2(b)), all privacy sensitive (*S*) users choose to opt-out; privacy non-sensitive (*NS*) users with low valuation choose to opt-in and purchase the product; and privacy non-sensitive *NS* users with high valuation choose to opt-out and buy the product. On the contrary, when α is low (Figure 2(b)), all privacy sensitive users choose to opt-out and not buy while all privacy non-sensitive users choose to opt-in and buy.


Privacy Sensitive (α)
Out-Not-Buy
Privacy Non-Sensitive ($1-\alpha$)
In-Buy
0
1
$P_{out}^{b^*} + c \geq 1$
Privacy Sensitive (α)
Out-Not-Buy
Out-Buy
Privacy Non-Sensitive ($1-\alpha$)
In-Buy
Out-Buy
0
1
$P_{out}^{b^*} + c = \dfrac{1+c}{1+\alpha}$

(a) $0 \leq \alpha \leq c \leq 1$

(b) $0 \leq c < \alpha \leq 1$

Figure 2. Illustration of Benchmark Equilibrium

Lemma 1 *(Benchmark). In the equilibrium without PDPs under high privacy concerns α, the proportion of opt-in users is decreasing in privacy concern (α) but increasing in search cost (c). $P_{out}^{b^*}$, π^{b^*} and total social welfare are decreasing in privacy concern (α) and search cost (c). User surplus is increasing in privacy concern (α) but decreasing in search cost (c).*

Lemma 1 is the result of the trade-off faced by the seller when he makes pricing decisions for opt-out users. The seller's profits come from two markets: an opt-in market which consists only of privacy non-sensitive (*NS*) users and an opt-out market which includes both privacy sensitive (*S*) and privacy non-sensitive (*NS*) users. An increase in the proportion of privacy sensitive users α will directly shrink the opt-in market which makes the marginal benefit of decreasing a unit of P_{out} (i.e., making more users to opt-out and buy) surpass the marginal cost (i.e., less users to opt-in and buy). Thus the optimal P_{out} decreases and the opt-out market indirectly expands. However, the profit loss from a smaller opt-in market cannot fully be compensated by the small profit gain from the opt-out market, which contributes to a lower total profit . An increase in search cost makes opt-in a more attractive choice, in other words, the marginal user between opt-in and opt-out will shift right immediately (i.e., a higher marginal valuation). It makes the marginal benefit of reducing P_{out} excess the marginal cost of reducing P_{out} which slightly drives down the optimal P_{out}. The profit gain from the opt-in market expansion cannot compensate for the loss from the shrinkage of the opt-out market. Thus, the total profit goes down.

PDP with Naïve Users

In this section, we consider a monopolistic seller who can employ privacy dark pattern (PDP) practices facing only naïve users. In other words, they will be successfully tricked by PDP designs such that there is no credibility loss for the seller. We denote it using superscript *n*. Users' utilities were presented in Table 1. The timing of game is depicted in Figure 1. Similarly, we use backward induction to derive the equilibrium.

Stage 4: Buying – Since the additional cost d imposed by PDP practice is a sunk cost (i.e., as long as users choose to opt-out, there will be a cost d irrespective of any purchase decision), opt-in and opt-out users' purchase behavior is identical to the one in the benchmark case. Regardless of their privacy cost, opt-in users whose valuation is greater than $P_{in}(v)$ and opt-out users whose valuation is bigger than $P_{out} + c$ will purchase the product.

Stage 3: Pricing $P_{in}(v)$ and P_{out} – Following the same logic of the benchmark model, the seller has no incentive to charge a higher or lower price than v for the opt-in user with product valuation v. Therefore, we have:

$$P_{in}^{n^*}(v) = v \tag{4}$$

Again, in order to derive the optimal uniform price P_{out} for opt-out users, let us first analyze users' information disclosure behavior in stage 2.

Stage 2: Opt-in/Opt-out – Given the pricing strategy for opt-in users in stage 3, users would like to maximize their utility in Table 1 by choosing to either opt-in or opt-out. As can be seen, privacy non-sensitive (*NS*) users will either choose to "Opt-in and Buy" or "Opt-out and Buy." Privacy sensitive (*S*) users' purchase behavior depends on the size of PDP level d and the privacy cost r. If d is small ($d < r$), *S* users will choose to "Opt-out and Buy" or "Opt-out and Not-buy." It is similar to the benchmark case. There will be some privacy sensitive (*S*) users that are not covered by the market. However, when d is high enough ($d \geq r$), "Opt-out and Not-buy" is an invalid choice for *S* users and they will choose to either "Opt-in and Buy" or "Opt-out and Buy." In this case, both *S* and *NS* users will buy the product. The additional cost d imposed by the PDP hedges out the privacy cost r.

Stage 1: PDP Level – Obviously, the seller will set a large enough PDP level d (i.e., $d \geq r$) such that all users will choose to opt-in which is similar to the world where users have no choice but to opt-in. It empowers the seller to conduct first-degree price discrimination to all users. All users will opt-in and purchase the product.

Lemma 2 *(Solution with Naïve Users). When users are naïve and the seller has the ability to utilize privacy dark pattern practices, the equilibrium is characterized as:*

- $P_{in}^{n^*}(v) = v$
- $P_{out}^{n^*} \geq 1 - c - d + r$
- $d^{n^*} \geq r$
- *All users choose to opt-in and buy*

In the equilibrium, the seller earns a profit $1/2$ while the total user surplus is $-\alpha r$. Compared to the benchmark, the presence of privacy dark patterns increases seller's profit but decreases user surplus. The change of total social welfare depends on the magnitude of privacy cost r. This naïve users case models the world where users have no choice but to opt-in or users do not really care about PDP practices. For instance, before the era of privacy, individuals have to accept the privacy policy (aka, share all personal information) before they can visit a website.

PDP with Sophisticated Users

In the previous section, users are naïve such that they will passively accept the additional cost d imposed by PDP designs. In other words, there is no cost for the seller to employ a high level of PDP practices. That is the reason why the seller will set a extremely high d in the equilibrium. Nevertheless, increasing privacy concerns make users more sensitive to the PDP design in the era of privacy. Users will identify the presence of PDP practices and might distrust the seller when the PDPs level is high. Therefore, in this section, we investigate the potential drawback of setting high PDP levels for the seller when users are sophisticated. Users are sophisticated such that they can recognize and negatively react to the presence of PDPs which would incur credibility loss for the seller.

In our model, we model the loss of trustworthiness by assuming that the market size will shrink by λd when the seller sets PDP level at d. In other words, a λd proportion of users will directly choose to "Opt-out and Not-buy" regardless of the following prices ($P_{in}(v)$ and P_{out}). The new potential market size is $(1-\lambda d)$ rather than 1 when the seller chooses a PDP level d. The parameter λ represents users' sensitivity to the presence and darkness of PDPs. For simplification, we normalize λ to 1 in our analysis.

We denote the solution for the sophisticated users model using the superscript s. According to the similar logic, the seller will set:

$$P_{in}^{s^*}(v) = v \tag{5}$$

Therefore, the seller faces the following profit function given a combination of $(P_{out},\ d)$:

$$\pi(P_{out},\ d) = \left[\alpha\pi^{S}(P_{out}, d) + (1-\alpha)\pi^{NS}(P_{out}, d)\right](1-d) \tag{6}$$

There is a trade-off for the seller when he decides the level of PDP. On the one hand, a high PDP level d increases users' opt-in rate which expands the opt-in market in two ways: transferring low valuation privacy sensitive (*S*) users from "Opt-out and Not-buy" to "Opt-in and buy" and transferring high valuation users (both *S* and *NS* users) from "Opt-out and Buy" to "Opt-in and Buy." Apart from this ***market division effect***, there is also a ***market shrinkage effect*** $(1-d)$. A higher PDP level will hurt users' trustworthiness. The loss of market size is increasing in PDP level d.

Lemma 3 presents how the seller's pricing strategy $P_{out}^{s^*}$ and PDP strategy d^{s^*} depend on the privacy concern α, reduced search cost c and privacy cost r. First of all, for any $(\alpha,\ c) \in (0,\ 1) \times (0,\ 1)$, when privacy cost r is low, similar to the naïve users case, the seller will set a high P_{out} (where $\underline{P_{out}} \geq 1 - c$) and high PDP level d (where $d = r$) such that all users (both *S* and *NS* users) choose to opt-in and buy the product. In this case, the market division effect dominates the market shrinkage effect. Secondly, when the privacy cost r is high, the market shrinkage effect will dominate the market division effect. The seller will choose a more conservative PDP strategy. In particular, when privacy concern α is high and the search cost is relatively low (area I), or privacy concern α is low and the search cost c is relatively high (area IV), the seller prefers ***to not utilize any privacy dark pattern designs*** $(d = 0)$ which is similar to the benchmark case. The market force is strong enough to incentivize the seller to be privacy friendly. Nevertheless, when both privacy concern α and search cost c are high (areas II and III), the seller will choose a moderate P_{out} and d.

Lemma 3 *(Solution with Sophisticated Users). When users are sophisticated and the seller has the ability to utilize privacy dark pattern practices, the equilibrium is characterized as Table 3 and Figure 3.*

r	$(\alpha,\ c)$	$P_{out}^{s^*}$	d^{s^*}	$P_{in}^{s^*}(v)$
Low $r \in [0,\ \overline{r}_i]$	All Areas	$\geq 1-c$	r (Use PDP)	v
High $r \in (\overline{r}_i,\ 1]$	area I	$\dfrac{1-\alpha c}{1+\alpha}$	0 (No PDP)	
	Area II	$\dfrac{1-\alpha c}{1+\alpha}$	x_4 (Use PDP)	
	Area III	$1-c-x_1$	x_1 (Use PDP)	
	Area IV	$\geq 1-c$	0 (No PDP)	

Table 3. Equilibrium with Sophisticated Users[5]

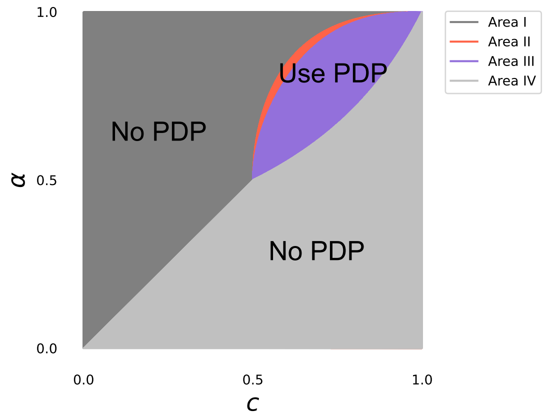


Figure 3. Equilibrium with Sophisticated Users Under High Privacy Cost

Impact of PDP

In order to examine the impact of PDP intervention, we compare our benchmark equilibrium with one from the naïve users model and one from the sophisticated users model.

Proposition 1 *(Impact of PDPs). With the presence of PDPs, users are weakly worse off while the seller is weakly better off.*

When users are naïve, the seller will choose a high P_{out} and d such that all users have no choice but to opt-in and buy the product. Privacy sensitive users will get a utility of $-r$ while privacy non-sensitive users will receive 0 utility. The seller extracts all user surplus. The seller is strictly better off with the presence of PDP when users are naïve. According to Figure 2, privacy sensitive users are strictly worse off and privacy non-sensitive users are weakly worse off with the presence of PDPs when users are naïve.

When users are sophisticated, the seller is weakly better off since, in the worst case, he can abandon PDP to achieve the same profit as the benchmark without PDP. Our analysis shows that, regardless of the magnitude of α, c and r, users are weakly worse off with the presence of PDP. Nevertheless, the change in total social welfare depends on the magnitude of α, c and r.

Regulation on PDPs

With increasing concerns over the proliferation of PDPs, the public has recently called for regulation over PDPs (CNIL 2019; EDPB 2022; FTC 2021). It is commonly believed that PDPs should be fully prohibited as they go against users' best interests. In the previous section, our results have shown that the introduction of PDPs indeed makes users weakly worse off. However the presence of PDP could paradoxically increase total social welfare due to the market division effect. In this section, we consider a social planner who aims to maximize total social welfare by regulating PDP practices. In stage 1, the social planner will set a PDP level d to maximize social welfare rather than the seller deciding d to maximize its profit.

Proposition 2 *(Socially Optimal PDP Level). A social welfare maximizing planner will choose the following PDP level:*

$$d^{w^*} = \begin{cases} 0, & if \quad \overline{r} < r \leq 1 \\ r, & if \quad 0 \leq r \leq \overline{r} \end{cases}$$

Proposition 2 shows that, the social planner should fully ban the PDP practice only when the privacy cost r is high enough – the cutoff value relies on the combination α and c. Nevertheless, the socially optimal PDP level is ***non-zero*** when r is low enough. In other words, the presence of PDP practices increases social welfare when the privacy cost r is low. The reason is that setting $d = r$ will convert those privacy sensitive users with low valuation who originally choose to "opt-out and not buy" when $d = 0$ into "opt-in and buy". These gain from more consumption utility will dominate the loss from privacy sensitive users' privacy loss when r is low.

Welfare Analysis

Lemma 3 depends considerably on privacy concern α, search cost c and privacy cost r. Thus, changes in these parameters have consequences on user surplus (CS), profits (π) and total social welfare (TW). Based on lemma 3, we conduct static comparative analysis with respect to α, c and r.

Comparative Statics for α

Lemma 4 *(Effects of Privacy Concern α). Raising the proportion of privacy sensitive users α among the population has the following effects on users surplus, seller's profits, and social welfare (ceteris paribus):*

r	$(\alpha,\ c)$	$\frac{\partial CS}{\partial \alpha}$	$\frac{\partial \pi}{\partial \alpha}$	$\frac{\partial TW}{\partial \alpha}$
Low $r \in [0,\ \overline{r}_i]$	All Areas	-	0	-
High $r \in (\overline{r}_i,\ 1]$	area I	+	-	-
	Area II	+	-	+
	Area III	-	-	-
	Area IV	0	-	-

Table 4. Effect of Users Privacy Concern α

Lemma 4 shows that the impacts of α on user surplus, profit and total social welfare depend on r and c. When the privacy cost r is low, both user surplus and social welfare are decreasing in α while the seller's profit is independent of α. This can be attributed to the seller's PDP and pricing strategies: $(P^{s^*}_{out}, d^{s^*}) = (\underline{P_{out}}, r)$ under which the seller has extracted all users' surplus from the market of potential users $(1 - d^{s^*})$. The loss of users' surplus and social welfare come from more privacy sensitive users' (higher α) privacy loss.

When the privacy cost r is high, the seller's profit is deceasing in α while the effects of changing α on user surplus and social welfare depend on c. For (α, c) in area I, the optimal PDP level is 0 and the price for opt-out users is decreasing in α. The positive user surplus only comes from the consumption utility from those users (both *S* and *NS* users) with high valuation who choose to opt-out and buy the product. Therefore, in this case, user surplus is increasing in α. Increasing α makes more privacy sensitive users uncovered by the market which contributes to a lower social welfare. Nevertheless, for (α, c) in area II, both user surplus and social welfare are increasing in α. On the contrary, both users surplus and social welfare are decreasing in α when (α, c) is in area III. Finally, when (α, c) is in area IV, the optimal PDP level is 0 and the price for opt-out users is high enough such that all privacy sensitive users choose to opt-out and not-buy while all privacy non-sensitive users choose to opt-in and buy which contribute to a 0 user surplus. Thus, user surplus is independent of α while social welfare is decreasing in α since the seller's profit is decreasing in α.

Comparative Statics for r

Lemma 5 *(Effects of Privacy Cost r). Raising the privacy cost r has the following effects on user surplus, seller's profits, and social welfare (ceteris paribus):*

r	$\frac{\partial CS}{\partial r}$	$\frac{\partial \pi}{\partial r}$	$\frac{\partial TW}{\partial r}$
Low $r \in [0,\ \overline{r}_i]$	-	-	-
High $r \in (\overline{r}_i,\ 1]$	0	0	0

Table 5. Effect of Privacy Cost r

Lemma 5 shows that when the privacy cost r is low, user surplus, seller's profits and social welfare are decreasing in r. Nevertheless, when it is high enough, user surplus, profits and social welfare are independent on r.

Comparative Statics for c

Lemma 6 *(Effects of Search Cost c). Raising the search cost c has the following effects on user surplus, seller's profits, and social welfare (ceteris paribus):*

r	$(\alpha,\ c)$	$\frac{\partial CS}{\partial c}$	$\frac{\partial \pi}{\partial c}$	$\frac{\partial TW}{\partial c}$
Low $r \in [0,\ \overline{r}_i]$	area I,II,III,IV	0	0	0
High $r \in (\overline{r}_i,\ 1]$	area I	-	-	-
	area II	-	-	-
	area III	+	-	+
	area IV	0	0	0

Table 6. Effect of Search Cost c

Lemma 6 shows that when the privacy cost r is low, or high and (α, c) is in area IV, user surplus, seller profits and social welfare are independent of search cost c. Nevertheless, when the privacy cost r is high and (α, c) is in area I or II, users surplus, seller profits and social welfare are decreasing in search cost c. Finally, when the privacy cost r is high and (α, c) is in area III, seller profit is decreasing while both user surplus and social welfare are increasing in search cost c.

Conclusion

In this paper, we present a game-theoretic model consisting of a monopolistic seller who engages in privacy dark pattern practices and heterogeneous users who decide whether or not to disclose their personal information. Our results show that users are worse off and the seller is better off when the seller uses PDPs. Nevertheless, the seller is incentivized to choose not to embrace PDP designs when the privacy cost is high and the ratio of privacy concern and reduced search cost is either too high or too low. In other words, market forces could be strong enough to achieve a no PDP design world. However, in most cases, the seller will adopt some level of PDP designs. Especially, when users' privacy cost is low enough, the seller will employ a high enough PDP practice. A welfare maximizing social planner would allow positive PDP designs when users' privacy cost is sufficiently low.

There are several limitations in our current study that call for additional future research. Firstly, in our model, we assume that the seller can perfectly infer opt-in users' valuations. Other signal structures have also been documented in the literature. For example, Koh et al. (2017) assume that the seller can only predict the participating users' true valuation with probability β and gain no new information with probability $1-\beta$. Future research could be conducted using other signal structures. Secondly, in our model, we assume that the seller can employ first degree price discrimination for opt-in users. Future study could check whether or not our main results hold if the seller can only charge a uniform price for opt-in users. Finally, in our model, we assume that both privacy sensitive users and privacy non-sensitive users respond the same to PDP design (aka, sharing the same PDP sensitivity λ). Future research could investigate the case where privacy sensitive users and privacy non-sensitive users have different PDP sensitivities λ^S and λ^{NS}. In addition, for simplification, we normalized λ to 1. The robustness of our results with respect to different values of λ are warranted.

Acknowledgments

This research was partially supported by a grant from the Singapore Ministry of Education Academic Research Fund Tier 1, R-253-000-158-114. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not reflect the views of the Singapore Ministry of Education or the Singapore Government.

References

Acquisti, A., Taylor, C., and Wagman, L. 2016. "The Economics of Privacy". *Journal of Economic Literature* (54:2), pp. 442–492.

Ali, S. N., Lewis, G., and Vasserman, S. 2023. "Voluntary Disclosure and Personalized Pricing". *The Review of Economic Studies* (90:2), pp. 538–571.

Aribarg, A. and Schwartz, E. M. 2020. "Native Advertising in Online News: Trade-offs among Clicks, Brand Recognition, and Website Trustworthiness". *Journal of Marketing Research* (57:1), pp. 20–34.

Armstrong, M. and Zhou, J. 2022. "Consumer Information and the Limits to Competition". *American Economic Review* (112:2), pp. 534–77.

Bösch, C., Erb, B., Kargl, F., Kopp, H., and Pfattheicher, S. 2016. "Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns". In: *Proceedings on Privacy Enhancing Technologies*, pp. 237–254.

Brownlee, J. 2016. *Why Dark Patterns Won't Go Away*. Available at: https://www.fastcompany.com/3060553/why-dark-patterns-wont-go-away.

CCPA 2022. *Text of Proposed Regulations*. Available at: https://cppa.ca.gov/regulations/pdf/20220708_text_proposed_regs.pdf.

Chellappa, R. K. and Shivendu, S. 2007. "An Economic Model of Privacy: A Property Rights Approach to Regulatory Choices for Online Personalization". *Journal of Management Information Systems* (24:3), pp. 193–225.

Choi, W. J., Jerath, K., and Sarvary, M. 2020. "Advertising and Price Competition Under Consumer Data Privacy Choices". Working Paper, Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3708273.

CNIL 2019. *Shaping Choices in the Digital World*. Tech. rep. Available at: https://linc.cnil.fr/sites/default/files/atoms/files/cnil_ip_report_06_shaping_choices_in_the_digital_world.pdf. Commission Nationale Informatique & Libertés.

Dengler, S. and Prüfer, J. 2021. "Consumers' Privacy Choices in the Era of Big Data". *Games and Economic Behavior* (130), pp. 499–520.

Di Geronimo, L., Braz, L., Fregnan, E., Palomba, F., and Bacchelli, A. 2020. "UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception". In: *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pp. 1–14.

EDPB 2022. *Guidelines 3/2022 on Dark Patterns in Social Media Platform Interfaces: How to Recognise and Avoid them*. Tech. rep. Available at: https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf. European Data Protection Board.

Frobrukerrådet 2018. *Deceived by Design, How Tech Companies Use Dark Patterns to Discourage Us From Exercising Our Rights to Privacy*. Tech. rep. Available at: https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf. Norwegian Consumer Council.

FTC 2021. *Bringing Dark Patterns to Light: An FTC Workshop*. Available at: https://www.ftc.gov/news-events/events/2021/04/bringing-dark-patterns-light-ftc-workshop.

Goode, S., Hoehle, H., Venkatesh, V., and Brown, S. A. 2017. "User Compensation as a Data Breach Recovery Action: An Investigation of the Sony PlayStation Network Breach". *MIS Quarterly* (41:3), pp. 703–727.

Hann, I. H., Hui, K. L., Lee, S. Y. T., and Png, I. P. 2008. "Consumer Privacy and Marketing Avoidance: A Static Model". *Management Science* (54:6), pp. 1094–1103.

Hidir, S. and Vellodi, N. 2021. "Privacy, Personalization, and Price Discrimination". *Journal of the European Economic Association* (19:2), pp. 1342–1363.

Hu, M., Momot, R., and Wang, J. 2022. "Privacy Management in Service Systems". *Manufacturing & Service Operations Management* (24:5), pp. 2761–2779.

Ichihashi, S. 2020. "Online Privacy and Information Disclosure by Consumers". *American Economic Review* (110:2), pp. 569–95.

Ichihashi, S. 2023. "Dynamic Privacy Choices". *Microeconomics* (15:2), pp. 1–40.

Koh, B., Raghunathan, S., and Nault, B. R. 2017. "Is Voluntary Profiling Welfare Enhancing?" *MIS Quarterly* (41:1), pp. 23–44.

Lin, T. 2022. "Valuing Intrinsic and Instrumental Preferences for Privacy". *Marketing Science* (41:4), pp. 235–253.

Luguri, J. and Strahilevitz, L. J. 2021. "Shining a Light on Dark Patterns". *Journal of Legal Analysis* (13:1), pp. 43–109.

Mathur, A., Acar, G., Friedman, M. J., Lucherini, E., Mayer, J., Chetty, M., and Narayanan, A. 2019. "Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites". In: *Proceedings of the ACM on Human-Computer Interaction*, pp. 1–32.

Mathur, A., Kshirsagar, M., and Mayer, J. 2021. "What Makes a Dark Pattern... Dark? Design Attributes, Normative Considerations, and Measurement Methods". In: *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pp. 1–18.

Nouwens, M., Liccardi, I., Veale, M., Karger, D., and Kagal, L. 2020. "Dark Patterns After the GDPR: Scraping Consent Pop-ups and Demonstrating Their Influence". In: *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pp. 1–13.

Wu, Y., Gal-Or, E., and Geylani, T. 2022. "Regulating Native Advertising". *Management Science* (68:11), pp. 8045–8061.