PRIVACY PROTECTION:
PETS BY INDIVIDUALS, PDPS BY FIRMS

by

CHEN DAWEI

A dissertation submitted for the degree of

DOCTOR OF PHILOSOPHY

in

INFORMATION SYSTEMS AND ANALYTICS

DEPARTMENT OF INFORMATION SYSTEMS AND ANALYTICS

NATIONAL UNIVERSITY OF SINGAPORE

2023

Supervisor:
Professor Jungpil Hahn

Examiners:
Dr Jin Chen
Dr Um Sungyong

Declaration

I hereby declare that this thesis is my original work and it has been written by me in its entirety. I have duly acknowledged all the sources of information which have been used in the thesis.

This thesis has also not been submitted for any degree in any university previously.

Dawei Chen

Chen Dawei

11 September 2023

To My Family, Advisor and Friends

Acknowledgments

This has been a difficult, winding and unforgettable journey. Starting from endless reading of papers and tough coursework, the journey took its first step into the vast sea of academic research. Meanwhile, the plentiful and intensive seminar series made me stay at the forefront of academic research. In the beginning, the coursework and seminars were quite challenging for a non-native English speaker like me. Even though the term projects from coursework have been excruciating, it became even more exhausting when I started my very first study, which became the first essay in this dissertation. Picking up a solid and huge research topic – information privacy – is never a wise choice. A comprehensive literature review, endless brainstorming, continuous reconceptualizing the phenomenon and successive framing of the research questions made it take over two years to finish the first draft of the first study. Unfortunately, it was more challenging when I started my second, analytical modeling study. The research question was only finalized after three proposals were brutally shot down which took more than a year and a half. It was the hardest time! I would like to express my sincere gratitude to all those who have helped and supported me throughout my PhD journey.

First and foremost, my sincere and hearty thanks and appreciations go to my dissertation advisor, Professor Jungpil Hahn, for his guidance, support, and encouragement throughout my research. Professor Hahn has been an excellent mentor and has provided invaluable advice and feedback on my work. I have learned a lot from our weekly individual meetings: how to conduct the literature review, how to conceptualize a novel research question, how to construct an integrated research framework, how to answer a research question in the scientific way, how to present a research paper, etc. I have been equipped with all skills and knowledge to be an independent researcher under the supervision of such a great advisor! Particularly, he is so supportive and patient during the hardest time in which I struggled with the proposal of the second study for around two years! Words are powerless to express my gratitude.

Secondly, I would also like to thank the members of my thesis committee, Drs. Jin Chen and Um Sungyong, for their insightful comments and suggestions, which have greatly improved the quality of my research. In addition, I am grateful to the examiners of my graduate research paper, Drs. Heng Cheng Suang and Vaibhav Rajan, for their constructive comments on my first study. Furthermore, I am grateful to the staff and faculty of the Department of Information Systems and Analytics at NUS School of Computing, who have created a stimulating and supportive academic environment.

Thirdly, I would like to extend my thanks to my colleagues in our great Garbage Can Lab, Zhou Junjie, Li Junyi, Li Yonggang, and Muhammad Nauman Shahid for their comments and support in our lab meetings. And my warm gratitude also goes to my best friends, Wang Hao and Wang Jieyu, for their support and encouragement during the hardest time. Special thanks to Wang Hao who has helped me a lot in the mathematical parts of the second study.

Finally, I would like to express my heartfelt appreciation to my family for their unwavering love, encouragement, and support throughout my PhD journey. Without their support and encouragement, this achievement would not have been possible.

Contents

Abstract

Advances in data collection and mining techniques have given rise to the necessity of privacy protection. Apart from privacy regulations, individuals and firms also play considerable roles in the process of privacy protection. For example, to combat the threat of privacy invasion, individuals are proactively adopting privacy enhancing technologies (PETs) to protect their personal information. For enterprises, it takes great effort and resources, such as privacy dark patterns (PDPs) practices, for them to “wisely” comply with privacy regulations. This dissertation seeks to understand the role individuals and firms play in the process of privacy protection through two studies.

The first study examines the impact of end-user PETs on firms’ analytics capabilities. After a comprehensive review of end-user PETs, we propose an inductively derived framework which qualitatively shows that end-user PETs induce measurement error and/or missing values with regards to attributes, entities, and relationships in firms’ customer databases, but the impact of specific end-user PETs may vary by analytics use case. We propose a value-oriented framework through which firms can study and quantify the impact of end-user PETs. We illustrate the value of this framework by applying it with simulation experiments in the context of product recommendations that quantitatively find that consumers’ adoption characteristics (i.e., adoption rate and pattern) and PETs protection characteristics (i.e., protection mechanism and intensity) significantly affect the performance of recommender systems. In addition, our results reveal the presence of spillover effects. In the presence of end-user PETs adoption, not only PET users but also non-users become worse off; moreover, PET users suffer more in term of recommendation accuracy. Even though observations from PET users are problematic, we find that their removal could actually further deteriorate recommendation accuracy.

The second study investigates the economic implications of privacy dark patterns (PDPs) through which firms could “wisely” play privacy protection games. It is commonly believed that PDPs advantage firms by deceiving and collecting more information from consumers. Nevertheless, they could also hinder firms’ credibility and consumers might stop sharing information to and purchase products from firms. Thus, the second study, firstly, aims to examine whether PDPs always benefit firms and hurt consumers. We also try to answer whether market force is sufficient to keep PDPs at low levels. Our results show that the presence of PDPs indeed makes 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 the reduced search cost of opt-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 shrinkage when the seller increases its level of PDPs. Finally, we show that a welfare maximizing social planner would allow the presence of PDPs when the users' privacy cost is sufficiently low.

This dissertation contributes to the privacy protection literature from two perspectives. Firstly, we propose a framework, both qualitatively and quantitatively, to understand the data impact of end-user privacy enhancing technologies (PETs) adopted by individuals. Secondly, we uncover the economic implications of privacy dark patterns (PDPs) and their regulation.

List of Figures

List of Tables

Chapter 1

Introduction

"If this is the age of information, then privacy is the issue of our times."

– Acquisti et al. (2015)

If data is the new oil of the digital economy, privacy invasion is the new climate change. The mining of data has given rise to an increasing extent of privacy invasion. The recent advances of data mining techniques (i.e., machine learning, artificial intelligence, deep learning, etc.) accelerate this new "climate change." The number of reported data breaches and the number of exposed records are keeping at all time highs in recent years. A recent survey reveals that 79% of US adults reported being not too or not at all confident that firms would use their personal information in ways they will feel comfortable with and that firms will admit mistakes and take responsibility if they misuse customers' personal information (Auxier et al. 2019). Therefore, it is urgent to propose new regulations or better understand the market forces to internalize and reduce the negative externalities (i.e., privacy invasion) induced by new oil (data) usage (Acquisti et al. 2016).

Privacy protection is the key to new oil (data) extraction and reduce climate change (privacy invasion). Since GDPR went into effect in 2018, the dynamic and high-developing privacy ecosystem has witnessed the rise of new privacy legislations in different countries around the world. It is reported that 71% countries in the world have already put in place legislation to protect their citizen privacy [1]. These privacy regulations are continuing to evolve in breadths and depths. Their focus has moved from traditional personal information privacy protection to more complex

[1] Data from https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

and emerging contexts (i.e., AI, IoT, metaverse, Web3, etc.) and new kinds of personal information (i.e., health data, biometric data, genetic data, etc.). They have laid a solid foundation on the general privacy protection principle and shed light on more specific requirements. There is no doubt that these privacy laws have increased consumers' privacy awareness and have forced companies, especially, big tech firms, to change their data practices. However, regulation alone is not a ideal one-stop solution to the complex privacy protection challenge. After the first great excitement when GDPR went into effect in 2018, people have grown frustration with GDPR's limitation (i.e., enforcement problem) (Burgess 2022). Apart from the prominent role of privacy regulation, individuals and firms also play considerable roles in the process of privacy protection.

Individuals (i.e., data subjects) are proactively defending themselves against invasion of privacy through the active adoption of end-user privacy enhancing technologies (PETs). The market has witnessed an increasing number of and increasing adoption of PETs – the number of daily user connections to the Tor network, the carrier of the dark web network and one of the most prominent PETs in the world, is currently approximately 2 million[2]; ad-blocker penetration rate among US Internet users has reached 40% (Blockthrough 2021); with GDPR going into effect, consumers are now explicitly asked to consent to cookies when they visit websites.

From the firms' perspective, the adoption of PETs by individuals would affect the data that they collect. For example, an online retailer like Amazon.com might record a consumer's IP address incorrectly when they are using the Tor browser for online shopping at its online storefront. Another example is the recent change in Apple's iOS that gives users the ability to block the sharing of their device's identifier for advertisers (IDFA) with app publishers. This change makes it difficult for publishers and advertisers to track users and as a result will hamper the effective targeting of advertisements and could lead to significant financial loss for firms whose value creation heavily rely on the data related to the tracking of consumer behaviors. As the quality of an organization's data is a key component of firms' analytics capabilities (Gupta and George 2016), this study asks whether and how

[2] See https://metrics.torproject.org/userstats-relay-country.html for Tor usage metrics.

end-user PETs might affect firms' analytics capabilities.

Although PETs have recently gained much momentum and considerable academic efforts have been made from computer science to investigate the technical design and implementation of specific PETs (Danezis and Gürses 2010, Diaz and Gürses 2012), our understanding of the economic value and impact of PETs or how consumers' adoption of various types of PETs might affect firms' value creation is still limited (Acquisti et al. 2016). Therefore, our first study aims to examine the impact of end-user PETs on firms' analytic capabilities.

In our first study, we propose a data-oriented framework that shows that end-user PETs fundamentally introduce missing values and/or measurement error with regards to attributes, entities and relationships in firms' customer database. This insight allows us to develop a value-oriented framework of end-user PETs that articulates how firms can conceptualize and quantify how consumers' adoption of PETs will impact their value creation. Simulation results in the context of product recommendations find that the adoption of end-user PETs can negatively affect firms' recommendation accuracy. The impact heavily depends on consumer's adoption behavior (i.e., the extent of adoption and what types of consumers are more likely to adopt) and PET characteristics (i.e., how the PET alters the data and by how much). Interestingly, we find that there is a significant spillover effect – the adoption of PETs could decrease the recommendation accuracy even for PETs non-users. Furthermore, we show that it is not a good idea for firms to simply delete all (corrupted) data from PETs users.

On the other side, to achieve those sophisticated and different privacy right empowered by the privacy regulations, it is necessary for the firms (i.e., data collectors) to provide proper infrastructures. During the infrastructure engineering process, firms can "wisely" play the privacy compliance game by employing privacy dark patterns (PDPs). PDPs refer to interface design practices which influence consumers to disclose information that they do not intend to disclose. They are prevalent in the era of privacy. For example, Nouwens et al. (2020) showed that around 90% of surveyed websites in the UK which contain consent management features adopt different extents of PDP practices. These PDP practices include implicit consent, making rejecting all tracking cookies more difficult than accepting all cookies, and pre-ticked (i.e., enabled by default) checkboxes, among others. The

European Data Protection Board (EDPB) identified a list of PDP practices in the context of social media platforms, namely, *overloading*, *skipping*, *stirring*, *hindering*, *fickle*, and *leaving in the dark* (EDPB 2022).

Even though PDPs have recently gained great momentum, the prominent focus of this literature still focus on descriptive aspects, namely, on its definition (Mathur et al. 2019), taxonomies of PDPs (Mathur et al. 2021), how prevalent they are (Di Geronimo et al. 2020, Nouwens et al. 2020) and their effectiveness (Luguri and Strahilevitz 2021). Our second study aims to investigate the economic implications of privacy dark pattern (PDP) practices through which firms could "wisely" play the privacy protection game. It is commonly believed that PDP advantages firms by deceiving and collecting more information from consumers. Nevertheless, it could also hinder firms' credibility and consumers might stop sharing information to and purchase products from these firms. Given this trade-off, we firstly seek to answer: *Do privacy dark pattern (PDP) practices always benefit the data controller and hurt the data subjects?* Given the deceptive nature of PDPs and their potential disadvantage for consumers, the public and the government have called for the banning of PDPs in practice. Thus, our second study also seeks to answer: *Are market forces (i.e., competition) sufficient to keep PDP practices at a relative low level*? Or *What is the optimal regulation over privacy dark pattern practices?*

We build a game-theoretic model to answer the above research questions. In the benchmark model setup, a monopoly seller offers a single product to many consumers. The seller chooses the level of PDP practices to influence users' information disclosure behavior. After observing the information provided by consumers, the seller decides the pricing strategy which in turn determines consumers' purchase decision. Our results shows that the presence of privacy dark pattern practices indeed make users weakly worse off while the seller is weakly better off. Nevertheless, the seller has incentive to not utilize any privacy dark pattern practices when users' privacy cost is high and the ratio of privacy concern and the reduced search cost of opt-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 gains from making more users opt-in (i.e., disclose personal information) will be outweighed by the loss from the total market shrinkage as the seller increases the level of PDPs. Finally, we shows that a social welfare maximizing social planner would allow the presence of PDP when the users' privacy cost is sufficiently low.

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

Taken together, this dissertation aims to examine the economic implications of privacy protection from two perspectives. The first study provides rich implication for firms to understand and handle the data challenge induced by end-users PETs adopted by individuals. The second study provides implications for digital businesses to employ privacy dark pattern and for policy makers for the regulation on PDPs.

Chapter 2

Impact of End-user PETs

2.1 Introduction

Consumer data is increasingly being regarded as the most valuable asset for companies. There is no doubt that mining of consumer data has become a powerful engine of value creation for firms (McAfee and Brynjolfsson 2012). By exploiting vast flows of consumers' personal information, firms can gain a better understanding of their customers' preferences and valuations which facilitates more efficient targeting, offering of more relevant advertising, and/or the provision of personalized services to improve the acquisition, retention and growth of customers (Acquisti et al. 2016). Naturally, high quality and large quantity of consumer data is imperative for firms' value creation. Therefore, in an effort to leverage the inherent value in consumer data, enterprises have made great investments to collect, store and analyze as much high-quality consumer data as they can handle.

Given the substantial value that can be generated from personal information, companies are collecting different kinds of and vast amounts of personal information by hook or by crook. The brutal and reckless plunder of individuals' personal information and lack of adequate protection give rise to extensive privacy concerns [1], not only with respect to the organization that collected the data with consent and through legitimate means but also due to potential data breaches whereby a

[1] It is challenging to define "privacy" universally. Smith et al. (2011) provided an excellent debate on "what is (and is not) privacy". Acquisti et al. (2016), Tucker (2022) summarized the definition and conceptualization of privacy in the area of economic. In our work, privacy refers to the right of individuals' control over what kind of their personal information is collected by whom and used for what purpose.

malicious actor may gain access to that organization's data. The number of reported data breaches and the number of exposed records are keeping at high levels in recent years. A recent survey reveals that 79% of US adults reported being not too or not at all confident that firms would use their personal information in ways they will feel comfortable with and that firms will admit mistakes and take responsibility if they misuse customers' personal information (Auxier et al. 2019).

To combat the threat of increasing privacy invasion, scholars from various disciplines (e.g., law, economics, computer science, information systems, etc.) are calling for more research on and solutions for privacy protection (Acquisti et al. 2016, Bélanger and Crossler 2011, Smith et al. 2011). In general, approaches to privacy protection can be classified into two types – regulation and self-regulation (Bennett and Raab 2020). Recently, a number of sophisticated and strict data privacy regulations (e.g., GDPR in Europe 2018, CCPA in California 2018, PIPL in China 2021, ADPPA in USA 2023) have been proposed all over the world. These regulations comprehensively specify different individuals' privacy rights and firms' responsibilities to protect consumers' privacy. There is no doubt that these privacy laws increase consumers' privacy awareness and force companies, especially, big tech, to change their data practice. However, it is not a one-stop ideal solution to the complex privacy protection challenge. After the first great excitement when GDPR went into effect in 2018, people have grown frustration with GDPR's limitation (i.e., enforcement problem) (Burgess 2022).

Given the limited effectiveness of privacy laws and firms' self-regulation, consumers are proactively defending themselves against invasion of privacy. For instance, 55% of American adults prefer better tools for allowing them to personally control their private information over stricter laws to help safeguard personal data (Auxier et al. 2019). As a result, various end-user privacy enhancing technologies (PETs), which refer to IT artifacts protecting informational privacy by eliminating or minimizing personal data by individuals (van Blarkom et al. 2003), are playing an increasingly more prominent role. The market has witnessed an increasing number of and increasing adoption of PETs – the number of daily user connections to the Tor network, the carrier of the dark web network and one of the most prominent PETs in the world, is currently approximately 2 million[2]; ad-blocker penetration rate among US Internet users has reached 40% (Blockthrough 2021); with GDPR going into effect, consumers are now explicitly asked to consent to cookies when they visit websites.

From the firms' perspective, the adoption of PETs by individuals would affect the data that they collect. For example, an online retailer like Amazon.com might record a consumer's IP address incorrectly when they are using the Tor browser for online shopping at its online storefront. Another example is the recent change in Apple's iOS that gives users the ability to block the sharing of their device's identifier for advertisers (IDFA) with app publishers. This change makes it difficult for publishers and advertisers to track users and as a result will hamper the effective targeting of advertisements and could lead to significant financial loss for firms whose value creation heavily rely on the data related to the tracking of consumer behaviors. As the quality of an organization's data is a key component of firms' analytics capabilities (Gupta and George 2016), this study asks whether and how end-user PETs might affect firms' analytics capabilities.

Although PETs have recently gained much momentum and considerable academic efforts have been made from computer science to investigate the technical design and implementation of specific PETs (Danezis and Gürses 2010, Diaz and Gürses 2012), our understanding of the economic value and impact of PETs or how consumers' adoption of various types of PETs might affect firms' decision making and performance is still limited (Acquisti et al. 2016). In this study, we offer a novel perspective to conceptualize the value implications of end-user PETs for firms. If more and more consumers are adopting end-user PETs to protect their privacy, then what are the implications for firms whose value creation heavily depends on collecting and analyzing consumers data? Should managers be concerned when more and more consumers are adopting PETs? At what point (of extent of adoption) should firm start to be concerned? How can firms mitigate such concerns? What kinds of technologies or practices may counteract the threat of data quality degradation resulting from PETs adoption?

To gain a deeper understanding of the relevant issues and offer some answers

[2] See https://metrics.torproject.org/userstats-relay-country.html for Tor usage metrics.

to the above questions, we need to first understand how different end-user PETs alters the data that is collected by firms. We therefore conduct a comprehensive review of end-user PETs by reviewing both the relevant academic literature as well as surveying existing technologies used in practice to systematically understand and classify what kinds of PETs are currently available to individuals (i.e., *what* of end-user PETs) and how different types of end-user PETs might alter enterprise data (i.e., the *how* of end-user PETs). Based on this classification, we develop a theoretical framework of end-user PETs that focus on the impact of various end-user PETs on the nature of the data challenges that firms will face based on how end-user PETs alter (i.e., deteriorate) the data that is being collected. Given that the value implications of end-users' PETs adoption would depend on the nature of the analytics a firm conducts using their collected data, we propose an analytical framework to think about how to quantify the value implication of end-user PETs adoption. We illustrate this framework by applying it to a common business analytics use case of product recommendations using customer product ratings data. This helps to better understand when firms should start to be concerned about the adoption of PETs by their consumers (i.e.,the *when* of end-user PETs).

Based on the comprehensive review of end-user PETs, our proposed data-oriented framework shows that end-user PETs could introduce missing value and/or measurement error with regards to attributes, entities and relationships in firms' consumer database. Moreover, based on our value-oriented framework of end-user PETs, the simulation results in the context of product recommendation find that the adoption of end-user PETs could negatively affect firms' recommendation accuracy. The impact heavily depends on consumer's adoption behavior (adoption rate and adoption pattern) and PETs characteristics (protection mechanism and protection intensity). Interestingly, we find that there is a spillover effect – the adoption of PETs could decrease the recommendation accuracy for PETs non-users. Furthermore, we show that it is not a good idea for firms to delete all corrupted data from PETs users.

Our study contributes to the literature on privacy enhancing technologies (PETs) in several meaningful ways. First, from a theoretical standpoint, we provide a framework of end-user PETs which not only qualitatively conceptualizes the impact of those existing end-user PETs, but also serves as a useful tool to anticipate emerging and new end-user PETs in the future. Second, our proposed analytical framework and approach offer organizations tools that can be immediately applied to better understand and plan for the potential detrimental impacts of end-user PETs adoption. Our numerical illustration quantitatively provides specific and significant practical implications for firms to understand the extent of potential impact of end-user PETs. In particular, we study how the consumers' adoption behaviors (e.g., adoption rate, adoption patterns) and the characteristics of end-user PETs (e.g., protection intensity, protection mechanism) might influence a firm's analytics performance in the context of product recommendations. Finally, based on both the above qualitative and quantitative analysis, we also discuss the implications for firms to mitigate the potential negative impact of end-user PETs.

2.2 Related Work

2.2.1 Privacy Enhancing Technologies

Privacy enhancing technologies (PETs), which are defined as "a system of ICT measures protecting informational privacy by eliminating or minimizing personal data thereby preventing unnecessary or unwanted processing of personal data, without the loss of the functionality of the information systems" (van Blarkom et al. 2003, p. 33), have attracted abundant attention from academics and practitioners in recent years. Due to the rapid expansion of the Internet and increasing significance of privacy protection, research on PETs has dramatically progressed. Here, we provide a brief overview of the extant literature.

A first stream of research which is from computer science mainly studies the functional design requirements of specific PETs. Principles of anonymity and pseudo-anonymity have been proposed to design better PETs for various use cases (e.g., email, online communication, location data sharing, etc.) following Pfitzmann and Waidner (1987) who investigated three types anonymous communication: sender anonymity, receiver anonymity and unlikability of sender and receiver. Numerous algorithmic techniques (e.g., k-anonymity (Sweeney 2002), l-diversity (Machanavajjhala et al. 2007), t-closeness (Li et al. 2007), differential privacy (Dwork 2008), etc.) have been proposed to achieve a desired level of anonymity in the context of data sharing for enterprises. Similarly, anonymous networks, such as the mix network (Chaum 1981), the DC network (Chaum 1988) and the Onion routing network (Reed et al. 1998), have been developed to lay the foundation for ensuring anonymous communication in a variety of contexts. In addition, control (Whitley 2009) and transparency (Janic et al. 2013), or consent and inform, are other vital and widely used privacy design mechanisms. This stream of literature, however, mainly focused on enterprise PETs that help firms to safeguard their internal data by producing shareable privacy-protected data. However, this stream of research does not concern itself with the quality of the data (or, implicitly assumes that companies have already collected high quality consumer data) but focuses on ensuring that their data management approaches are privacy-preserving.

A second stream of research focuses on the general classification of various PETs. Various scholars have proposed classification frameworks to better understand the landscape of PETs. Heurix et al. (2015) provided a taxonomy which can be used as a tool for the systematic comparison of different PETs. In addition, Danezis and Gürses (2010) and Diaz and Gürses (2012) classified PETs based on the three different concepts of privacy, namely, privacy as *control*, privacy as *confidentiality*, and privacy as *practice*. Fischer-Hbner and Berthold (2017) classified PETs into minimization PETs, transparency PETs and hybrid PETs. Additional reviews of classifications of PETs are provided in a report by London Economics (2010). Even though abundant prior classifications provide a general and nuanced picture of PETs from various perspectives, the impact of end-user PETs on firms has not been directly addressed.

Finally, a third stream of research investigates the impact of PETs. Goh et al. (2015) showed that consumers' subscription into Dot-Not-Call registries would increase subsequent registrations from others since unregistered users will be exposed to more marketing solicitations. The advent of ad-blockers was shown to decrease websites' content quality and advertising revenue (Shiller et al. 2018, Anderson and Gans 2011). Contrary to these negative impacts, some researchers showed that ad-blocker proliferation could be beneficial to publishers because of its discriminatory power (Aseri et al. 2020) and relaxed competition among publishers (Despotakis et al. 2021). Moreover, Chen and Liu (2021) proposed that a lower ad-blocker adoption cost could incentivize good advertisers to further increase the quality of their ads. As can be seen, much of the work investigating the impact of various kinds of end-user PETs have focused on ad-blockers. As a result, our knowledge of what and how significant the impact of different types of end-user PETs on firms is still limited.

2.2.2 Adversarial Machine Learning

Our work is also related to the literature of adversarial machine learning which studies "effective machine learning techniques against an adversarial opponent" (Huang et al. 2011, p. 43). In their seminal work, Barreno et al. (2006) categorized the malicious adversaries' attacks on machine learning systems according to three properties, namely, *influence* (whether attacks alter the training process), *specificity* (whether attacks alter a small set of points or a very general class of point), *security violation* (whether attacks introduce only false negative or both false negative and false positive error). After this taxonomy, the following research has documented factors affected an adversary's capabilities and countermeasures against attacks in various research contexts and machine learning algorithms (Huang et al. 2011, Kurakin et al. 2016).

Our research fits into the general framework of adversarial machine learning literature. The end-user PETs adopters are adversaries; various end-user PETs could introduces different attacks into firms machine learning algorithms. However, our work is different from the adversarial machine learning literature from two perspectives. Firstly, in our study, the aim of end-user PETs adoption is to protect individuals' privacy which unintendedly introduces attacks to firms machine learning algorithms rather than malicious attacks against machine learning algorithms in the adversarial machine learning study. Secondly, most importantly, our work aims to understand the data impact of various end-user PETs while the adversarial machine learning literature focus on general attacks on machine learning algorithms. In other words, the data impact from end-user PETs impact could go beyond machine learning model training.

2.3 A Review and Classification of End-user PETs

To uncover the impact of various end-user PETs, it is useful to first catalog what kinds of end-user PETs are available to individuals. To better understand the current landscape of end-user PETs, we conduct a comprehensive review consisting of a top-down review of the academic literature and as well as a bottom-up review from end-user PETs used in practice. The top-down review of the academic literature highlights existing classifications and their classification principles. However, it is also necessary to check whether there are new commercial technologies not captured by the academic literature due to the rapid development of end-user PETs. The combination of taxonomies from a top-down review of the academic literature and a bottom-up inductive classification of commercial technologies used in practice[3] offers a comprehensive exposition of end-user PETs.

Before presenting the results of our top-down and bottom-up reviews, we first outline the specific scope for our review as there are many related technologies that are not directly relevant to our current discussion of how end-user PETs might impact firms' analytics capabilities.

2.3.1 Scope of the Review

There are generally two broad categories of PETs, namely, end-user PETs and enterprise PETs. In particular, enterprise PETs, which refer to technologies adopted by firms to protect their customers' privacy, include various encryption techniques, such as homomorphic encryption (Armknecht et al. 2015) and searchable encryption (Abdalla et al. 2005); and different statistical disclosure control (or privacy preserving technologies) for data sharing and data mining, such as k-anonymity (Sweeney 2002), l-diversity (Machanavajjhala et al. 2007), t-closeness (Li et al. 2007), and differential privacy (Dwork 2008). As mentioned earlier, these enterprise PETs are controlled by firms and have little impact on firms' analytics performance since it is assumed

[3] For the bottom-up review, since the majority of end-user PETs exist in the form of applications and web browser extensions, we searched leading software applications stores, namely, the Apple App Store, the Google Play Store, and the Chrome Web Store, using the keyword "privacy". In addition, we also referred to the database of PETs from the Center for Internet and Society (CIS) (https://cyberlaw.stanford.edu/wiki/index.php/Main_Page.) and the list of end-user PETs from the Electronic Privacy Information Center (EPIC) (https://epic.org/privacy/tools.html.) to complement our list of PETs to review. After removing duplicate entries, a total of 354 unique end-user PETs were identified.

that firms have already collected high quality of consumer data and need to protect it against unwanted outside access. Therefore, enterprise PETs are excluded from our scope of review and we focus primarily on end-user PETs.

End-user security protection technologies are also excluded from the scope of our review. The concept of privacy and security are interrelated, and the terms are often used interchangeably in much of the literature. Ackerman (2004) asserted that security is a necessary but not sufficient condition for privacy. Despite the intersection and overlap, they are two distinct concepts (Dincelli et al. 2017). Security focuses on the protection of personal information with regards to integrity (i.e., information is not altered), authentication (i.e., data access requires authentication), and confidentiality (i.e., data can only be used by authorized people for authorized purpose) (Smith et al. 2011). Nevertheless, privacy protection focuses on the right of an individual to decide what information about themselves should be communicated to others and under what circumstances. In other words, security focuses on the protection of data from attackers and hackers, whereas privacy emphasizes what kind of data are collected for what purpose and by whom (Bansal 2017). Therefore, it seems that information security is a necessity for both individuals and firms and often guaranteed by enterprises since it is the firms' responsibility to protect their data from unauthorized users (e.g., hackers). The adoption of security technologies by individuals should also protect their information from hackers rather from firms. As a result, with respect to their interactions with firms, consumers are more concerned about the adoption of end-user privacy technologies rather than end-user security technologies. Therefore, it is vital for firms to understand the impact of the proactive adoption of end-user PETs.

2.3.2 A Review of PETs

We identified six categories of end-user PETs from our review of the academic literature and the bottom up inductive review of technologies available in practice. These include communication anonymizers, privacy setting, transparency enhancing technologies, trackers and evidences erasers, filters and blockers, and personal data stores which can classify all of the relevant end-user PETs reviewed. Definitions, examples, mechanisms and challenges faced by each category are discussed below.

The details of the whole review process are provided in the appendix

Communication Anonymizers. This category of end-user PETs comprises technological artefacts that protect users' IP address or other network addresses through anonymous communication networks (e.g., mixes and mix-network, onion network, garlic routing, etc.) enabling individuals to browse anonymously online (Danezis and Gürses 2010). These artefacts could be browsers (e.g., Tor, Epic), network layer (e.g., I2P), or search engines (e.g., lxquick, duckduckgo). They provide privacy protection by hiding or replacing one's real online identity (e.g., IP address, email address) with a non-traceable identity (e.g., a random IP address of hosts participating in the Tor network). They provide a high level of privacy protection in a convenient way making them the most adopted end-user PETs among the six categories. Unfortunately, these end-user PETs are oftentimes blocked by websites and suffer from slight slowdowns in the speed of browsing and communications. In addition, they are often critiqued for being the hotbed of illegal transactions (Biryukov et al. 2014). The bottom-up review identified 159 applications (44.92%) that fell into the category of communication anonymizers. These included virtual private networks (VPNs), firewalls, private search engines, fake/shared bogus email accounts, and social networks. Anonymization was achieved by primarily embedding into anonymous networks or proxies, adding noise or perturbation, using fake or virtual identities.

Privacy Settings. This category comprises tools embedded in smart phones, browsers and social media services, which, to some extent, can empower users to control who can access their personal information (Diaz and Gürses 2012). For example, privacy settings on Facebook allow individuals to limit what piece of personal information (e.g., age, gender, work, contact details, posts and comments) is visible to whom and check who has access to their online activities' information within third-party apps. The private browsing mode now common in web browsers (e.g., Incognito mode in Google's Chrome browser) is another example which asserts that no local trail (i.e., browsing history, HTTP cookies and passwords) would be stored on the user's computer by creating and deleting temporary sessions under private browsing. However, it will not prevent the service provider (i.e., the firm) from collecting a user's personal information that is not stored on their computer. In addition, the underlying mechanism of privacy setting is "control" which is heavily critiqued for only providing the illusion of control (Solove 2012), whereby individuals might share more sensitive information given that they feel more secure, which may ultimately lead to a more severe invasion of privacy (Brandimarte et al. 2013). We also identified 27 applications (7.63%) that can be classified as privacy settings technology in our bottom-up review. These included application that allow a user to view and control permissions required by various apps on their smartphone.

Transparency Enhancing Technologies. Transparency enhancing technologies (TETs) refer to tools which provide individuals with clear visibility of what kinds of personal information would be collected, how the information will be collected and processed subsequently. Fischer-Hbner and Berthold (2017) classified them into ex-ante and ex-post transparency enhancing technologies. The former, also referred to as policy checking technologies (Shen and Pearson 2011), are privacy policy creation and understanding tools that could be used in users' decision making and policy enforcement. For example, the Platform Privacy Preference (P3P) and the P3P privacy agent automatically compare users' personal privacy preferences against the full P3P policies of websites (Cranor 2003). Liu et al. (2016) proposed an intelligent agent called Personalized Privacy Assistant which is capable of learning individuals' privacy preferences and making decisions on behalf of its user. Ex-post TETs focus on transparency in regard to the processing of personal data after consumers have disclosed their personal information. An example is the Data Track project which allows individuals to view what kind of personal information has been collected by whom and for what purposes (Angulo et al. 2015). We identified 18 applications (5.08%) that fall under this category in our bottom up review. Most of these were privacy checkers that summarize various privacy policies or provide a privacy score or educational applications geared toward familiarizing users with basic privacy laws and general privacy-related knowledge.

Trackers and Evidences Erasers. This category comprises technologies which empower individuals to remove electronic traces of their online activities. Some tools (e.g., CCleaner) allow individuals to scan and delete browser search history and cookies from their computers. Some tools (e.g., Privacy Eraser) can even permanently remove information from an individual's hard disk by overwriting the content of the file so that even undelete programs will not able to recover it. Other premium tools (e.g., DeleteMe) provide stronger privacy protection by removing users' personal information from leading data brokers and people search sites. Even though these technologies indirectly protect individuals' privacy by deleting trackers from their own devices and evidences from some websites to avoid further unsanctioned data collection by firms, their protection capability is rather limited since service providers can easily insert new trackers and collect individuals' personal information again. The bottom-up review identified 50 applications (14.12%) in the category of trackers and erasers. These application allowed users to remove privacy-sensitive data, such as browsing history, cookies, adware, EXIF information from photos and sound files.

Filters and Blockers. This category comprises tools focused on preventing unwanted and unsolicited emails or messages and web-content from reaching individuals, such as ad blockers, cookies blockers and Do-Not-Track mechanisms. However, most filters and blockers are not considered to be privacy enhancing technologies since they only try to eliminate the post-hoc negative effect of the loss of privacy rather than preventing the loss of personal information in the first place. However, cookie blockers can to some extent protect privacy by blocking third-party cookies which can limit data collection by firms. Research has shown that publishers are increasingly employing anti ad-blockers to bypass ad-blockers. As a result, the impact of the presence of ad-blockers on stakeholders (individuals, advertisers, content providers) are still unclear (Aseri et al. 2020, Ray et al. 2017). The bottom-up review identified 100 applications (28.25%) that fall into this category of end-user PETs. These included application that block third-party advertisements (e.g., pop-ups and video ads), unwanted content, as well as various trackers, etc.

Personal Data Stores. Personal data stores (PDS) which refer to IT artefacts that allow individuals to manage and maintain their digital information (Van Kleek and OHara 2014) are believed to be the new and final solution to the issue of online privacy protection. Compared with traditional centralized data management system, PDS are structured in a decentralized way and empower individuals to fully control the collection and usage of their personal information. By assigning the property right of information to individuals and since all data is stored locally or at a trusted third-party location, the illegal collection and usage of sensitive data can be eliminated. Blockchain technology could achieve a fully decentralized personal data management system without requiring trusted third parties (Zyskind et al. 2015). Some examples of PDS are the Hub-of-All-Things (HAT), CitizenMe, and

Mydex. However, the design principles and technical structures of PDS are still in their infancy and as a result, we were not able to identify any PETs in practice that fall under this category.

The above comprehensive review provides a rich overview of the landscape of end-user PETs. Next, we develop a theoretical framework of end-user PETs that focuses on the impact of various end-user PETs on the nature of the data challenges that firms will face due to how they alter the data that is being collected.

2.4 A Theoretical Framework of End-user PETs

In this section, we develop a theoretical framework to help us better understand the impact of end-user PETs on firms' analytics capabilities. Our framework is divided into two parts – 1) we first articulate how different end-user PETs alter the data collected by firms; and 2) we conceptualize how changes in firms' data would result in deterioration in firms' use of analytics.

2.4.1 A Data-oriented Framework of End-user PETs

Fundamentally, end-user PETs alter the data collected by firms. For instance, the Tor browser, a popular end-user PETs, enables anonymity online and protects consumers' privacy by isolating each website a consumer visits so that third-party trackers and advertisers cannot track the consumers. This is done by randomly bouncing Internet traffic through a worldwide overlay network. The browser also automatically clears cookies and the browsing history when a consumer completes their browsing session so that websites cannot track the consumer across sessions. From the perspective of the firm collecting consumer data, what the Tor browser does is to provide a random client IP address for the consumer. Therefore, when the firm logs the consumer's IP address, the IP address that is stored will be different from the consumer's actual IP address and the firm's attempt to identify the consumer's location via IP geolocation lookup will yield incorrect results.

Therefore, we conceptualize the impact of end-user PETs on firms' data analytics capabilities as mediated by the changes in the firms' data. Conceptually, there can be two types of changes to the data: 1) omitting data values leading to missing

Figure 2.1: A Framework of End-user Privacy Enhancing Technologies (PETs)

	Measurement Error	**Missing Value**
Attributes	① shared bogus accounts, communication anonymizers	② privacy settings, personal data stores
Entities	③ shared bogus accounts	④ tracker erasers, transparency enhancing technologies
Relationships	⑤ shared bogus accounts	⑥ tracker erasers, transparency enhancing technologies

data, and 2) altering data values leading to erroneous data. Both types of data challenges are potentially detrimental to the accuracy of data analysis. According to the statistics literature, there are two common problems encountered during any data analysis – missing values and measurement error (Buonaccorsi 2010, Little and Rubin 2019). Missing values occur when no data value is recorded or stored for a variable or an observation. Measurement error refers to the differences between the measured or observed value of a quantity and its true value. The extant literature has shown that both missing value and measurement error could lead to bias and inefficiency in statistical estimation (Rubin 1976, Bound et al. 2001). Therefore, the measurement error and missing value challenges induced by end-user PETs may devastatingly affect firms' value creation by inducing incorrect inferences from their data analysis.

The challenges of measurement error and missing values induced by end-user PETs can occur with different kinds of data and at different stages of the data engineering pipeline, which may have different implications for firms. Ultimately, these two problems may occur in different elements in the dataset of an enterprise. In the relational data model (Codd 1970), a database is defined as a set of tuples (i.e., rows, records, objects, instances) organized into relations (i.e., entities, tables), described by attributes (i.e., columns, features), and where there are relationships among relations. In other words, there are three key elements that could be affected by missing values and/or measurement error from end-user PETs in the firms' data – i.e., entities, attributes and relationships. To sum up, we propose a 2 × 3 theoretical framework to highlight the impact of various end-user PETs on firms (see Figure 2.1). Examples of end-user PETs and the potential data problem induced by them in each cell are discussed below.

Cell ①: There is measurement error in attributes when some features of customers are incorrectly captured. In other words, values in some cells do not represent their true values. For instance, firms might record the wrong IP address if their consumers adopt a communication anonymizer. The use of shared bogus accounts will reflect completely incorrect demographic data for specific individuals. Therefore, firms will draw inaccurate inferences when analyzing consumer data due to its incorrectness. For example, firms might target the wrong consumer or provide irrelevant recommendations when the analytics models used to target and/or provide recommendations rely on customer demographic data.

Cell ②: There are missing values in attributes when end-user PETs obfuscate the data that is passed onto firms and as a result, values in some attributes are missing. For example, on social media, privacy sensitive individuals might choose to not make their posts public when they are given control over their information with PETs that support privacy settings. With personal data stores (PDS), if individuals have control over their digital information, privacy sensitive individuals will configure their PDS to only reveal non-sensitive data to firms leading to missing values in all attributes deemed sensitive. Data sparsity has been shown to significantly reduce the accuracy of recommendation systems (Grčar et al. 2005) or lead to biased coefficient estimations in the training of machine learning models if the mechanism of missingness is missing at random (MAR) or missing not at random (MNAR) (Rubin 1976).

Cell ③: There is measurement error in entities when for instance the same consumer is captured multiple times as "different" consumers in the firm's database, violating entity integrity of the relational database model. In other words, the same entity (e.g., a particular consumer) might be recorded as two or more different customers (or records). According to the universe of discourse (UoD) assumption, there should be a unique observed entity corresponding the actual entity in reality. Due to end-user PETs, enterprises might record a non-existent (i.e., fake) entity without a corresponding actual real entity, or incorrectly map an observed entity to another different entity. Shared bogus accounts would make firms collect the same or only one entity from multiple different actual entities who share the account.

Cell ④: There are missing entities as the firm cannot capture the information from some customers, in other words, there will be many missing (uncaptured) records. With transparency enhancing technology, individuals might be fully informed that a website do not respect their privacy and may no longer want to use this website. If trackers or cookies are effectively blocked, firms cannot collect any information from those consumers who adopt such blockers. With PDS, privacy sensitive consumers will configure them to not disclose their personal information. Bajari et al. (2019) have shown that the size of datasets significantly affects the accuracy of machine learning models. More importantly, if all privacy sensitive individuals are missing, enterprises could only capture information from those who do not care about their privacy, which will lead to severe selection bias.

Cell ⑤: Measurement error in relationships refer to the mismatch in joining records in a dataset. Theoretically, any measurement error in an entity's identifying attribute (i.e., primary or foreign key) would lead to measurement error in relationships. When a consumer A is observed and incorrectly recorded as consumer B, the relationship “consumer A ordered product X” would be recorded as “consumer B ordered product X”. With the use of shared bogus accounts, the true relationship “consumer A ordered product X; consumer B ordered product Y” could be recorded as “consumer C ordered product X and $\boldsymbol{Y}$. This problematic relationship would bias even simple summary / aggregation statistics and can significantly affect any analysis of associations. For example, with product recommendations, the performance of recommendation algorithms will be hampered since a particular consumer might be wrongly recommended products similar to some product when the consumer may not even have actually consumed or liked that product.

Cell ⑥: Missing values in relationships occur when the actual connections between records cannot be observed by firms. Since different tables are connected by foreign keys, missing values in foreign keys could induce this data problem.

For instance, when consumer A is not captured by firms, the relationship "consumer A orders product X" would be missing. Thus, firms' knowledge of consumer A is reduced or totally missing which also could influence any inferences from data analytics that rely on this association.

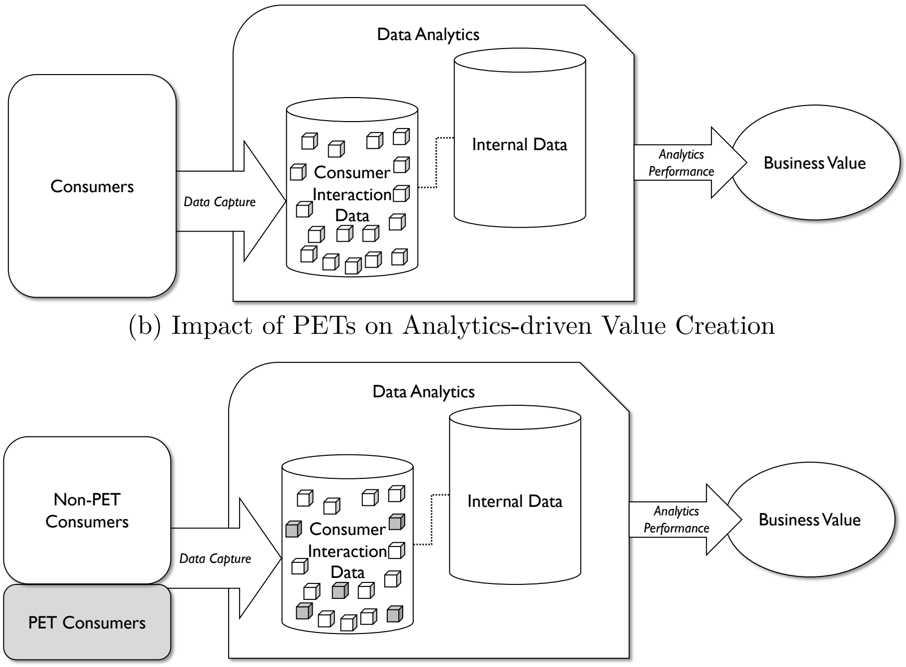
2.4.2 A Value-oriented Framework of End-user PETs

Our focus now shifts from understanding the "what" and "how" of end-user PETs to understanding the "when" of end-user PETs, or when should firms be concerned about the adoption of end-user PETs. Although the theoretical framework of end-user PETs (see Figure 2.1) developed above yields interesting conceptual insights into how the use of end-user PETs will impact the data collected by firms, it is still difficult to quantify the extent of this impact on firms' analytics performance. For a clearer conceptualization, we revisit the overall analytics-driven value creation process. Figure 2.2a summarizes the process of value creation from analytics of consumer data. Firms capture various data on consumers based on their interactions with the firms (e.g., consumers' purchase of the firms' products, clickstream data from the consumers' visits to the firms' website, consumers' responses to advertisements, consumers' engagements with the firms' social media contents, etc.). This data is integrated with the firms' other internal data (e.g., transaction data, product data, marketing data, etc.) and analytics is conducted on this data (e.g., predict a customer's purchase likelihood, identify products to recommend with greatest likelihood of cross-selling, etc.). Business value is generated when decisions and insights from the analytics are accurate.

Figure 2.2b highlights the impact of consumers' adoption of end-user PETs on firms' value creation. When consumers adopt end-user PETs, the data captured by firms on these consumers' interactions with the firm will be tainted with measurement error and/or missing values depending on the types of end-user PETs they use (see Figure 2.1). The tainted data will inevitably result in a degradation of analytics performance, which will lead to a reduction in business value. Therefore, the impact of end-user PETs on firms' business value creation can be conceptualized as the difference in business value between Figures 2.2b and 2.2a – i.e., $\textit{Impact of PETs} = \textit{Business Value}_{\text{no PETs}} - \textit{Business Value}_{\text{PETs}}$.

Figure 2.2: Impact of End-user PETs on Firms' Analytics Performance and Value Creation

(a) Analytics-driven Value Creation



(b) Impact of PETs on Analytics-driven Value Creation

As can be inferred from the above, the impact of PETs will vary based on 1) how the data collected by the firm is actually put into use (i.e., the analytics use case), 2) how the data collected by firms is tainted by the PETs, and 3) how many consumers are using PETs. We illustrate the application of this framework by applying it to one particular use case – product recommendations.

2.5 Case Study: Impact of End-user PETs on Product Recommendations

In this section, we apply our framework of the impact of end-user PETs on firms' analytics capabilities by studying how end-users' adoption of PETs affects a firm's production recommendation performance. We do so by simulating consumers' adoption of various end-user PETs at various extents to observe how the data inaccuracies (i.e., missing values and measurement errors) introduced by the PETs would impact the accuracy of product recommendations. Such a simulation-based approach has recently been used to study the longitudinal dynamics of recommender systems (Zhang et al. 2020).

2.5.1 Study Setup and Methodology

2.5.1.1 Data and Recommender Engine.

We studied the impact of end-user PETs on recommendation performance using the MovieLens 100k dataset[4] (Harper and Konstan 2015), which has been widely used in recommendation systems research. The MovieLens dataset consists of individuals' ratings for movies in the MovieLens website. All ratings are integer values between 1 and 5, where 1 represents the least liked items and 5 represents the most liked items. The minimum number of rating given by a user is 20 and the minimum number of rating for an item is 1. There are 943 unique users and 1,682 unique items resulting in a rating density of 6.31%.

We utilize the LensKit recommender package[5] to train the recommendation models. In particular, we use item-based collaborative filtering (CF) as our choice of recommendation algorithm since it is widely used in real world applications (e.g., product recommendations at Amazon.com) (Smith and Linden 2017). In the item-based approach, the original rating is mean-centered and normalized before calculating the similarity matrix, and the prediction of unknown rating for a user-item pair is calculated as the weighted sum of ratings received by the target item's neighbors where similarities are used as weights. We set the maximum number of neighbors to 50. We use the root mean squared error ($RMSE$) metric to evaluate the performance of the recommender system.

2.5.1.2 Factors Modeling.

As discussed in our value-oriented framework, the impact of end-user PETs on firms' analytics-driven value creation depends on how end-user PETs alter the firms' data, and which consumers are using the end-user PETs in interacting with the firms. The former can be broken down into 1) the type of data problem induced by end-user PETs (i.e., PETs protection mechanism) and 2) how severe the data

[4] The MovieLens dataset is available at https://grouplens.org/datasets/movielens/100k/.

[5] The LensKit package is available at https://lenskit.org.

altercations are (i.e., PETs protection intensity), and the latter can be broken down into 1) how many consumers are using end-user PETs (i.e., consumer PETs adoption rate) and 2) which consumers are using end-user PETs (i.e., consumer adoption patterns).

PETs Protection Mechanisms define the data problem induced by end-user PETs. As discussed in our theoretical framework, there are two kinds of data problems, namely, missing values and measurement error. In the context of product recommendations, if a user adopts an end-user PETs, their ratings may not be observed by firms (i.e., the "missing value" in entity; case ②) or their ratings may be attributed to another (or anonymous) user since their identity is concealed (i.e., the "measurement error" in relationships; case ⑤). In our simulations, for the missing case, we simply drop the PETs adopters' ratings; whereas for the measurement error case, we replace the user ID of the PETs adopters' observations' with a different (or new) user ID.

PETs Protection Intensity refers to the protection level of end-user PETs. If consumers adopt "ineffective" end-user PETs, firms might not concern themselves too much about this. As end-user PETs become more sophisticated, firms should be more concerned about users' adoption. In our simulations, we vary protection intensity by setting the proportion of the observations of an adopter of PETs to be "unprotected" or to have a data problem.

Consumer PETs Adoption Rate refers to the proportion of customers who have adopted end-user PETs to protect their privacy. Firms' data analytics performance will not be affected if there are very few users that have adopted any type of end-user PETs. However, if a large proportion of their customers have adopted end-user PETs, it will be challenging for firms to conduct any accurate estimation or prediction based on customer data with measurement error and/or missing values arising from their customers' use of end-user PETs. In our simulation, we we vary consumer PETs adoption rate by setting the proportion of all unique users in the dataset as end-user PETs users.[6]

[6] For both PETs protection intensity and consumer PETs adoption rate, we set the values to range from 10% to 70%, in increments of 10. We exclude those extreme cases where adoption rate and/or protection intensity are above 80% since they introduce too much randomness. The majority of the results are consistent even when those extreme cases are included. The case where adoption rate and protection intensity are 0% is also excluded since this is the same as the

Consumer PETs Adoption Pattern specifies who are more likely to be adopters of end-user PETs to explore the heterogeneity in users' privacy sensitivity. The adoption of end-user PETs cannot be assumed to be completely random. It is possible that those users who are more privacy sensitive might be more likely to adopt end-user PETs. It could also be that those who are more privacy-sensitive might be less likely to adopt end-user PETs (Ghose 2017). The literature has shown that the frequency of Facebook use is positively correlated with making modifications to privacy settings (boyd and Hargittai 2010). Users could increase their technological familiarity and privacy awareness as they consume online services with greater intensity. Therefore, heavy (i.e., frequent) users may be more likely to protect their personal information. On the other hand, privacy sensitive individuals may also be less likely to use online services. In other words, light (i.e., infrequent) users may be relatively more privacy sensitive. To study such heterogeneity in adoption, we experiment with three kinds of adoption patterns – i.e., uniform, light-sensitive and heavy-sensitive – by assigning a probability of being an adopter of end-user PETs according to users' usage intensity – in the context of product recommendations, rating frequency. In the "uniform" (baseline) case, all users are assigned the same probability of adopting the PETs; in the "light-sensitive" case, light users care more about their privacy and are more likely to adopt end-user PETs; finally, in the "heavy-sensitive" case, the adoption probability is positively correlated with the frequency of a user's ratings such that heavy users are more privacy sensitive and more likely to adopt end-user PETs.

2.5.1.3 Simulation Procedure.

The simulation process is summarized in Figure 2.3. We first split the dataset into train and test samples by timestamp. In other words, the earliest 80% of the observations comprise the training set whereas the latest 20% observations are in the test set. In addition, the test sample remain the same across all simulation experiments since on the one hand, firms typically utilize past observations to train the recommendation models and make predictions for the new coming users/observations using the trained models. On the other hand, having a consistent test sample would ensure that the results across experimental conditions are

benchmark case (i.e., no PETs case).

comparable. In total, there are 7 (adoption rate = $\{10\%, \dots, 70\%\}$) × 7 (protection intensity = $\{10\%, \dots, 70\%\}$) × 3 (adoption pattern = {light-sensitive, uniform, heavy-sensitive}) × 2 (protection mechanism = {missing value, measurement error}) = 294 experimental conditions. Each experiment is replicated 100 times in a Monte Carlo fashion to ensure that the results of the simulation reflect the underlying structure of the model rather than a particular realization of a stochastic process.

Figure 2.3: Simulation Procedure

Step 1: Set Benchmark

1.1. Split the dataset into train-test sample
1.2. Compute similarity matrix
1.3. Calculate item-user prediction
1.4. Evaluate benchmark recommendation performance

Step 2: Simulate PETs Adoption

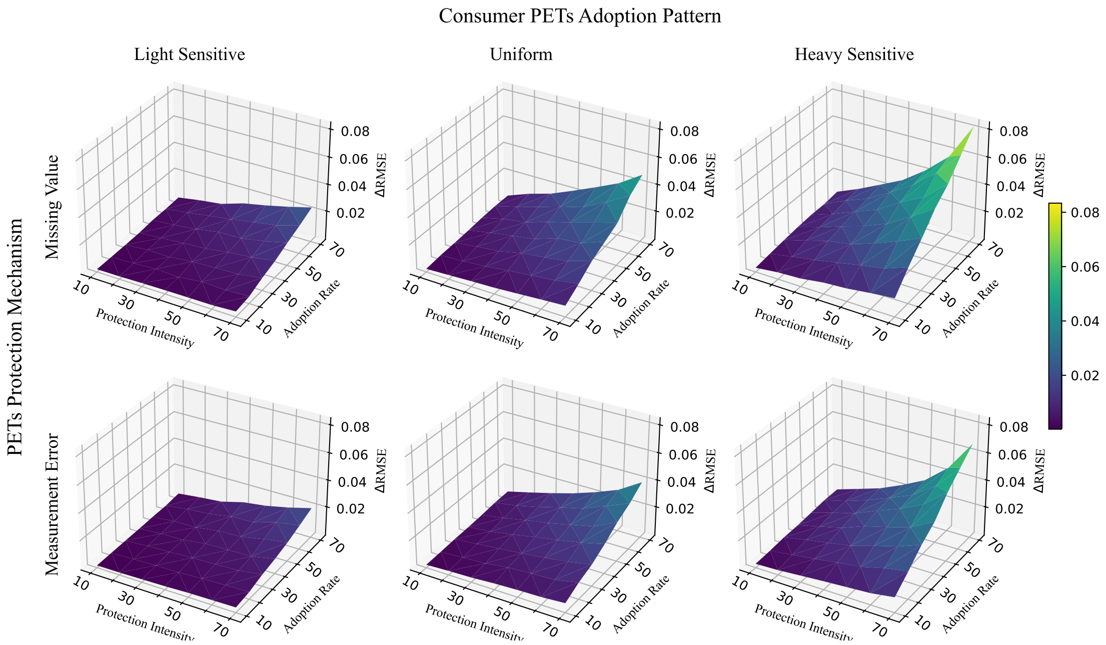
2.1. Assign adoption probability
2.2. Pick PETs users by adoption rate and adoption pattern
2.3. Introduce data problem by protection intensity and protection mechanism
2.4. Compute similarity matrix
2.5. Calculate item-user prediction
2.6. Evaluate recommendation performance

2.5.2 Results

The overall results of the simulations are summarized in Figure 2.4 which shows the increase in recommendation error (in terms of change in *RMSE* compared to the baseline of the no PETs case; $\Delta RMSE$) as a result of consumers' PETs adoption. Each 3-D chart shows the change in *RMSE* across varying levels of consumer PETs adoption rate (x-axis) and PET protection intensity (y-axis) for different consumer PETs adoption patterns (i.e., light-sensitive, uniform and heavy-sensitive; across columns of charts) and different PETs protection mechanisms (i.e., missing values vs. measurement errors; across rows of charts).

The results suggest that adoption rate and protection intensity significantly impact the performance of recommendation systems. The accuracy of recommendation decreases when consumers increasingly adopt end-user PETs to protect their privacy and when the level of protection from PETs intensifies. The impact of adoption rate and protection intensity are mutually reinforcing. However, when the adoption

Figure 2.4: Main Results



rate or protection intensity is low, the performance of the recommender system is still quite satisfactory, which is good news for firms. Among the three adoption patterns, performance is worst for the heavy-sensitive adoption case, followed by the uniform adoption case and then the light-sensitive case. The reason is that at the same adoption rate and protection intensity, more data would be hampered in the heavy-sensitive case as heavier users have more ratings (i.e., observations). The implication is that firms should care more about their more frequent customers.

Having ascertained through visual inspection of the results that the adoption of end-user PETs does have an impact on recommendation performance, we further scrutinize the results more quantitatively by conducting regression analysis of the simulation data. We investigate the impact of PETs characteristics (i.e., protection mechanism and intensity) and user characteristics (i.e., consumer PETs adoption pattern and rate) on the degradation of overall recommendation accuracy. We further study the externalities, or "spillover effects," in the recommendation performance degradation effect. Given that PETs users are the ones who generate tainted data to the recommendation algorithm, it makes sense that recommendation performance would be deteriorated for these consumers. However, the tainted data generated by the PETs users could also impact the recommendation accuracy for PETs non-users.

Therefore, we ask whether the impacts are uniform for all users or if they are more severe for PETs users (as compared with PETs non-users). Finally, we also study the effects of a possible mitigation strategy by firms. If we assume that firms have the ability to discern PETs users from PETs non-users, firms could try to maintain recommendation accuracy by dropping the product rating observations of PETs users. We study whether such a mitigation strategy would be effective. Table 2.1 provides the definitions of variables used in our regression analysis.

Table 2.1: Variables Definitions

Variables	**Definition**
Dependent Variables	
$\Delta RMSE$	The change in overall *RMSE* for all users in the test data between when PETs are used and the original dataset which is when PETs are not used
$\Delta RMSE_{use}$	The difference in *RMSE* between PETs users and non-users
$\Delta RMSE_{del}$	The change in *RMSE* if PETs users are identified and their observations are removed from the training sample
Independent Variables	
AdoptionRate	The proportion of PETs users among the whole population – i.e., 0.1, .., 0.7
ProtectionIntensity	The proportion of observations affected by the PETs among all observations for each PETs user – i.e., 0.1, ..., 0.7
Adoption	Indicator variables for adoption pattern; $Adoption_{HS} = 1$ and $Adoption_{LS} = 1$ for heavy-sensitive and light-sensitive adoption patterns, respectively; the baseline (i.e., $Adoption_{HS} = Adoption_{LS} = 0$) is for the uniform adoption pattern
Protection	Indicator variable for protection mechanism; $Protection_{MV} = 1$ for the missing value protection mechanism; the baseline (i.e., $Protection_{MV} = 0$) is for the measurement error protection mechanism

2.5.2.1 Impact of End-user PETs Adoption on Recommendation Accuracy

The overall impact of end-user PETs adoption on degradation of recommendation accuracy is summarized in Models 1 and 2 of Table 2.2. Model 1 includes only the main effects of the primary independent variables and Model 2 adds their interaction terms. The regression results reveal that the rate of adoption and level of protection intensity have negative effects on recommendation accuracy as can be inferred by the positive and significant coefficients of *AdoptionRate* ($\beta = 0.031$, $p < 0.01$) and *ProtectionIntensity* ($\beta = 0.038$, $p < 0.01$).[7] This is because more training data

[7] Given that the dependent variable $\Delta RMSE$ refers to the change in inaccuracy, a positive coefficient implies that an increase in the independent variable is associated with an increase in *in*accuracy, which we term a "negative" effect in terms of value as more inaccurate predictions are

Table 2.2: Regression Results

	$\Delta RMSE$		$\Delta RMSE_{use}$		$\Delta RMSE_{del}$	
$Variables$	(1)	(2)	(3)	(4)	(5)	(6)
$AdoptionRate$	0.031^{***}	0.027^{***}	-0.049^{***}	-0.002	0.092^{***}	0.012^{***}
	(0.000)	(0.000)	(0.004)	(0.007)	(0.002)	(0.001)
$ProtectionIntensity$	0.038^{***}	0.031^{***}	0.050^{***}	0.050^{***}	-0.045^{***}	-0.042^{***}
	(0.000)	(0.000)	(0.004)	(0.007)	(0.002)	(0.004)
$Adoption_{HS}$	0.008^{***}	0.007^{***}	-0.095^{***}	-0.094^{***}	0.083^{***}	0.080^{***}
	(0.000)	(0.000)	(0.002)	(0.003)	(0.001)	(0.004)
$Adoption_{LS}$	-0.006^{***}	-0.006^{***}	0.071^{***}	0.076^{***}	-0.017^{***}	-0.018^{***}
	(0.000)	(0.000)	(0.002)	(0.003)	(0.001)	(0.001)
$Protection_{MV}$	0.003^{***}	0.003^{***}	-0.002	0.002	0.003^{***}	0.001
	(0.000)	(0.000)	(0.002)	(0.003)	(0.001)	(0.001)
$AdoptionRate$ $\times ProtectionIntensity$		0.100^{***} (0.001)		0.026 (0.019)		-0.122^{***} (0.001)
$AdoptionRate$ $\times Adoption_{HS}$		0.015^{***} (0.000)		-0.192^{***} (0.009)		0.275^{***} (0.010)
$AdoptionRate$ $\times Adoption_{LS}$		-0.014^{***} (0.000)		0.039^{***} (0.009)		-0.055^{***} (0.005)
$AdoptionRate$ $\times Protection_{MV}$		0.007^{***} (0.000)		0.008 (0.007)		0.014^{***} (0.005)
$ProtectionIntensity$ $\times Adoption_{HS}$		0.028^{***} (0.000)		0.004 (0.009)		-0.040^{***} (0.004)
$ProtectionIntensity$ $\times Adoption_{LS}$		-0.019^{***} (0.000)		0.001 (0.009)		0.021^{***} (0.005)
$ProtectionIntensity$ $\times Protection_{MV}$		0.008^{***} (0.000)		-0.004 (0.007)		0.006 (0.005)
$Adoption_{HS}$ $\times Protection_{MV}$		0.002^{***} (0.000)		-0.001 (0.004)		0.007^{***} (0.004)
$Adoption_{LS}$ $\times Protection_{MV}$		-0.002 (0.000)		-0.010^{***} (0.004)		0.000 (0.002)
$constant$	0.011^{***}	0.011^{***}	0.015^{***}	0.013^{***}	0.003^{***}	0.004^{***}
	(0.000)	(0.000)	(0.002)	(0.002)	(0.001)	(0.001)
R^2	0.620	0.793	0.221	0.240	0.310	0.427
Observations	29, 400	29, 400	29, 390	29, 390	29, 400	29, 400

Significance Levels: $^{***}\, p < 0.01$; $^{**}\, p < 0.05$; $^{*}\, p < 0.1$

would be tainted as adoption rate and protection intensity are higher. This is consistent with Adomavicius and Zhang (2012) who showed that rating density and size had a positive impact on recommendation accuracy. With respect to patterns of PETs adoption, the results show that recommendation accuracy is deteriorated when heavy users are more likely to adopt PETs ($\beta = 0.008$, $p < 0.01$); whereas recommendation accuracy is actually improved if light users are more likely to be PETs users ($\beta = -0.006$, $p < 0.01$) when compared with the uniform adoption pattern case. Finally, when we compare the protection mechanisms of PETs, we see

less desirable.

that compared to PETs that introduce measurement errors, those that introduce missing data are more harmful to recommendation accuracy ($\beta = 0.003$, $p < 0.01$). In other words, reducing rating size (and thereby density) is more detrimental to having erroneous ratings in the similarity matrix.

When we investigate the interaction effects (see Model 2), we observe that most of the effects are mutually reinforcing – the negative impact of greater adoption rate on recommendation accuracy is stronger with greater protection intensity ($AdoptionRate \times ProtectionIntensity$: $\beta = 0.100$, $p < 0.01$); recommendation accuracy is also more severely deteriorated when heavy users are more likely to be PETs adopters if adoption rate is higher ($AdoptionRate \times Adoption_{HS}$: $\beta = 0.015$, $p < 0.01$) and also less severe when light users are more likely to be PETs adopters at higher adoption rates ($AdoptionRate \times Adoption_{LS}$: $\beta = -0.014$, $p < 0.01$); the more negative impact of the missing values protection mechanism (compared to the measurement error mechanism) was stronger with greater adoption rate ($AdoptionRate \times Protection_{MV}$: $\beta = 0.007$, $p < 0.01$). These effects are summarized and visualized in Figure 2.5. Overall these results offer statistical support for the earlier results based on visual inspection of the simulation results (see Figure 2.4).

2.5.2.2 Spillover Effects.

The above analyses investigate the impact of PETs adoption on overall recommendation accuracy for all users in the test sample and the results document that recommendation accuracy does indeed deteriorate when PETs are adopted by consumers and PETs protection intensity is greater. However, it is important to understand whether the degradation in recommendation accuracy applies to both PETs users (i.e., those who provide tainted data to the training of the recommendation algorithm) and PETs non-users (i.e., those that provide truthful data). In other words, are all users uniformly affected by the use of PETs by some users? Will PETs adopters be better or worse off than PETs non-users? To uncover these effects, we examine the differential impacts of PETs adoption on the recommendation accuracy for PETs users vs. PETs non-users. Figure 2.6 summarizes the results and Models 3 and 4 of Table 2.2 show the regression results with the difference in $RMSE$ of recommendation accuracy between PETs users and PETs non-users as the dependent variable (i.e., $\Delta RMSE_{use} = RMSE_{user} - RMSE_{non-user}$).

Figure 2.5: Impact of End-user PET Adoption on *RMSE*

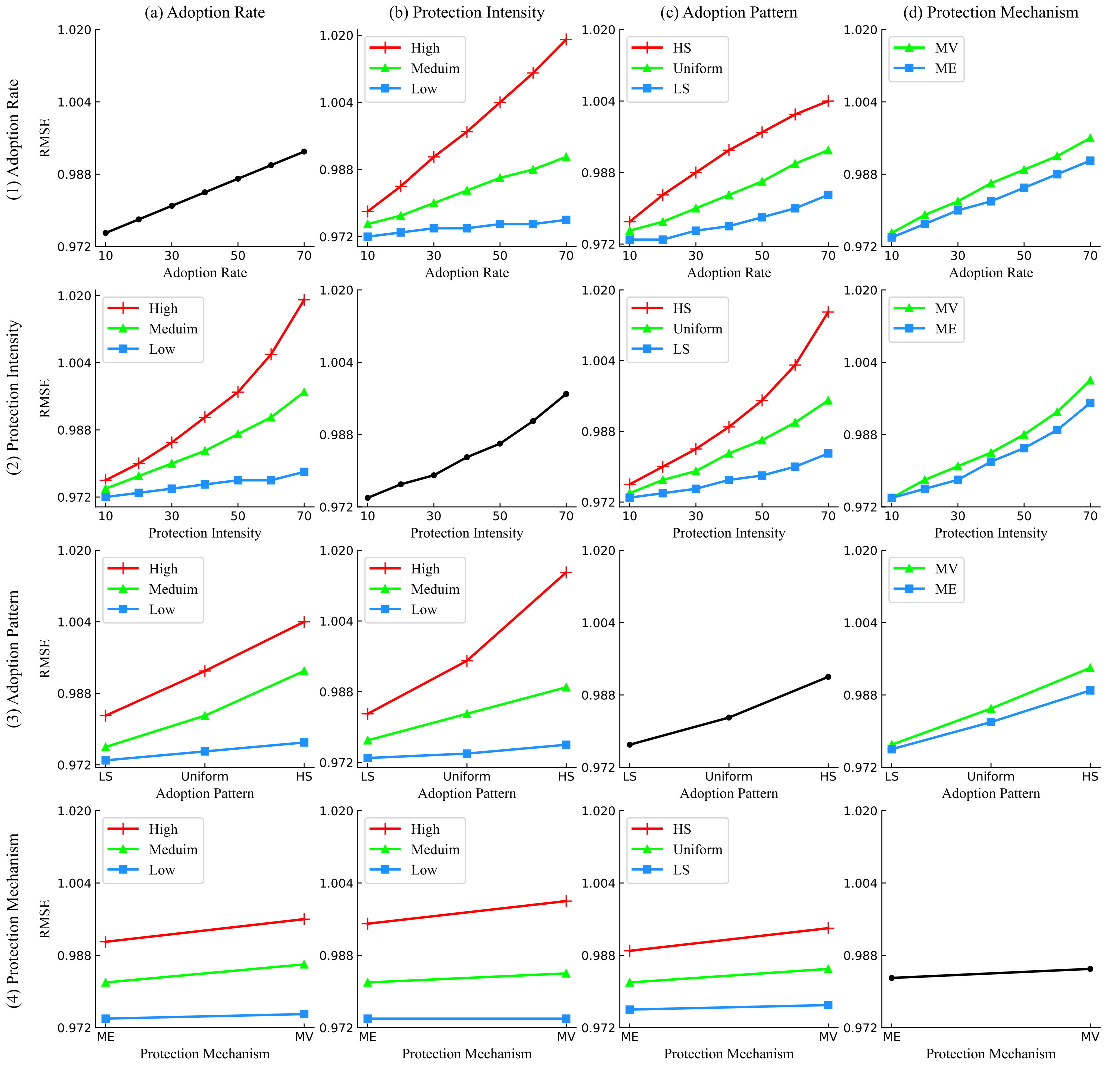
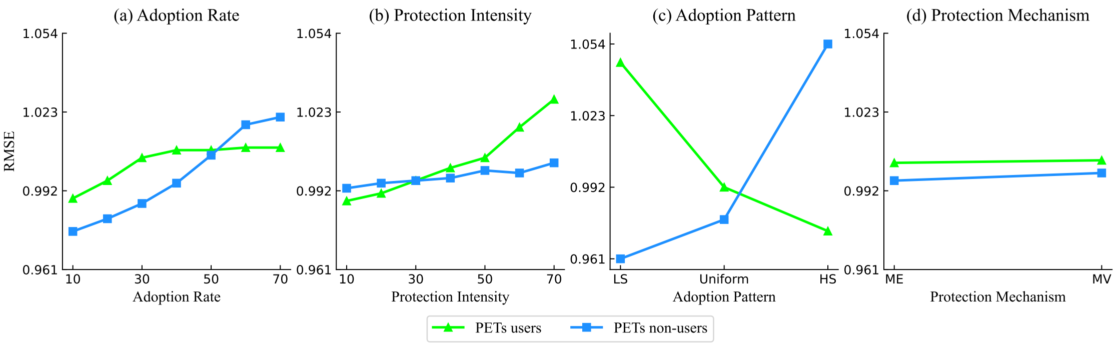


Figure 2.6: Comparison between PET users and PET Non-users



We first note that users of PETs are more worse off than non-users of PETs in terms of receiving less accurate recommendations (Model 3: *constant*: $\beta = 0.015$, $p < 0.01$). However, this is not because recommendation prediction accuracy is deteriorated only for PETs users – both PETs users and non-users become worse off as a result of PETs adoption from some consumers.[8] This can be attributed to the fact that a greater number of observations from PETs users' are tainted in the similarity matrix as compared to those from PETs non-users. Such a negative externality of privacy protection has been well documented in the privacy literature (e.g., Hann et al. 2008, Goh et al. 2015, Acquisti et al. 2016, Aseri et al. 2020) which showed that privacy sensitive users would be better off while other users would be worse since the privacy protection behaviors from privacy sensitive users would result in higher intensity marketing and advertising or higher prices for other (less privacy sensitive) users compared to privacy sensitive users. The reason is that privacy protection behaviors signal the consumers' segments which empowers firms to discriminate and make personalized offers. The negative externality here is somewhat different as both privacy sensitive users (i.e., those that use PETs) and privacy non-sensitive users (i.e., those that do not use PETs) are both subject to less accurate recommendations.

We also observe interesting dynamics with respect to the impact of PETs adoption and protection characteristics. The results show that although PETs users suffer more (compared to non-users) when adoption rate is low, this relationship is reversed when adoption rate is higher (see Figure 2.6a and Table 2.2, Model 3: $AdoptionRate$: $\beta = -0.049$, $p < 0.01$); greater protection intensity seems to lead to a stronger deterioration of recommendation accuracy for PETs users (see Figure 2.6b; $Protection\ Intensity$: $\beta = 0.0509$, $p < 0.01$); PETs users suffer more when light users are more likely to be the adopters whereas the non-users suffer more when heavy users are more likely to be the adopters of PETs (see Figure 2.6c; $Adoption_{LS}$: $\beta = 0.071$, $p < 0.01$; $Adoption_{HS}$: $\beta = -0.095$, $p < 0.01$); and PETs users suffer (slightly) more when the protection mechanism is one of measurement errors rather than missing values (see Figure 2.6c; $Protection_{MV}$: $\beta = -0.002$, $p < 0.01$).

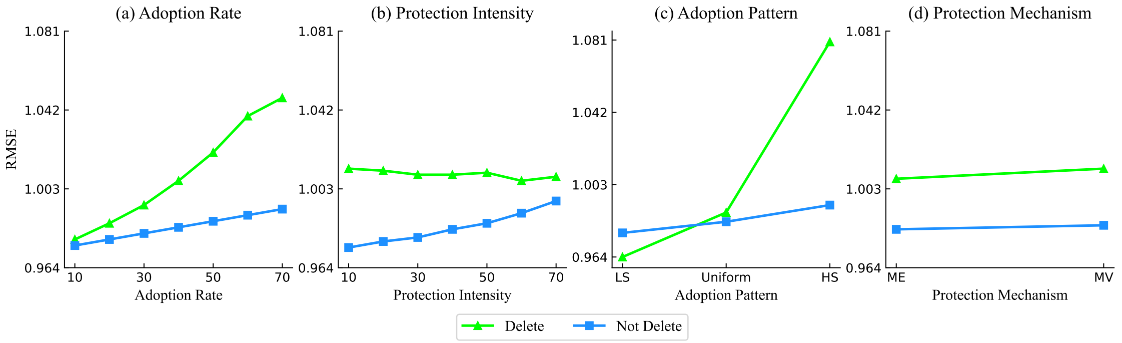
[8] Even in the case where $AdoptionRate = 0.1$ and $ProtectionIntensity = 0.1$, both the $RMSE$ for PETs users ($t = 107.03$, $p < 0.001$) and the $RMSE$ for PETs non-users ($t = 52.09$, $p < 0.001$) are significantly greater than the $RMSE$ from benchmark where there is no end-user PETs adoption.

However, the results of the interaction effects (see Model 4) suggest that the some of the above effects may be moderated by patterns of PETs adoption. For example, it is not the extent of adoption, per se, but what types of users who are more likely to adopt that moderates the impact of adoption rate on the difference in *RMSE* between PETs users and PETs non-users (Model 4: *AdoptionRate*: $\beta = -0.002$, *ns*). When heavy users are more likely to adopt PETs, recommendation accuracy is more severely deteriorated for those who do not use PETs (Model 4: $AdoptionRate \times Adoption_{HS}$: $\beta = -0.192$, $p < 0.01$). Conversely, when light users are more likely to adopt PETs, recommendation accuracy is more severely deteriorated for those who use PETs (Model 4: $AdoptionRate \times Adoption_{LS}$: $\beta = 0.039$, $p < 0.01$). We also observe that the main effects of PETs adoption pattern are significant and consistent in sign with the interaction effects with extent of adoption (Model 4: $Adoption_{HS}$: $\beta = -0.094$, $p < 0.01$; $Adoption_{LS}$: $\beta = 0.076$, $p < 0.01$), implying that greater extent of PETs adoption further amplifies the impact of adoption pattern. These results suggest that light users are more likely to suffer from deterioration in recommendation accuracy. Since if heavy users are more likely to adopt PETs, then the non-users of PETs (i.e., those who suffer from PETs in terms of deteriorated recommendation accuracy; see negative effect of $AdoptionRate \times Adoption_{HS}$ and of $Adoption_{HS}$) are more likely to be light users and if light users are more likely to adopt PETs, then the users of PETs (i.e., see positive effect of $AdoptionRate \times Adoption_{LS}$ and of $Adoption_{LS}$) are also likely to be light users. Similarly, with respect to the type of protection mechanism, PETs that introduce missing values (as opposed to those that introduce measurement errors) have a stronger detrimental impact on recommendation accuracy for PETs non-users when light users are more likely to adopt PETs (Model 4: $Adoption_{LS} \times Protection_{MV}$: $\beta = -0.010$, $p < 0.01$).

2.5.2.3 To Delete or Not To Delete.

Given the negative impact of PETs adoption by consumers on recommendation accuracy, we examine the possibility of one type of response strategy from firms – deleting problematic observations from PETs users in the training of the recommendation model. If firms have the ability to detect and identify PETs users, then, since PETs users introduce “tainted” data, firms might consider removing those corrupted observations from the training of the recommendation model in order to increase the

Figure 2.7: Comparison between Deleting and Not Deleting PET Users' Observations in Model Training



accuracy of recommendations. However, this strategy can lead to a deterioration of prediction accuracy as the size of the training dataset will be smaller. We investigate the efficacy of such a response strategy by comparing recommendation accuracy when PETs users' rating data are retained vs. removed from the training of the recommendation model.[9] Figure 2.7 summarizes the results and models 5 and 6 of Table 2.2 show the regression results with the difference in $RMSE$ of recommendation accuracy when PETs users' observations are removed from the training data as the dependent variable (i.e., $\Delta RMSE_{del} = RMSE_{del} - RMSE$).

Contrary to what firms might hope for in implementing this response strategy, the results show that removing "tainted" data from the training data actually hurts recommendation accuracy (Model 5: $constant$: $\beta = 0.003$, $p < 0.01$). As shown in Figure 2.7, except for when light users are more likely to adopt PETs, recommendation accuracy when PETs users' rating data is removed from the data is lower (i.e., greater $RMSE$) compared to when all users' (including both users *and* non-users of PETs) rating observations are used in the training of the recommendation model. This negative consequence is amplified when PETs adoption rate is greater ($AdoptionRate$: $\beta = 0.092$, $p < 0.01$) and when heavy users, as opposed to light users, are more likely to be the adopters of PETs ($Adoption_{HS}$: $\beta = 0.083$, $p < 0.01$; $Adoption_{LS}$: $\beta = -0.017$, $p < 0.01$). However, the negative consequence of the deletion response strategy is dampened as protection intensity is increased

[9] Naturally, if observations from PETs users are removed, the $RMSE$ for PETs users in the testing data will be 0 since there is no information on PETs users in the training sample. Therefore, in this section, we focus on the change in recommendation accuracy for PETs non-users after firms delete problematic observations from PETs users.

(*ProtectionIntensity*: $\beta = -0.045$, $p < 0.01$). Since protection intensity refers to the proportion of a user's data that is subject to manipulation (i.e., either missing or erroneous), deleting PETs users' observations at high levels of protection intensity implies that most of the deleted data are actually tainted, whereas at low levels of protection intensity, the firm would be deleting even correct (i.e., "untainted") data from PETs users.[10] The protection mechanism (i.e., missing values vs. measurement errors) only seems to have an impact when combined with other PETs adoption characteristics (Model 6: $Protection_{MV}$: $\beta = 0.001$, *ns*; $AdoptionRate \times Protection_{MV}$: $\beta = 0.014$, $p < 0.01$; $Adoption_{HS} \times Protection_{MV}$: $\beta = 0.007$, $p < 0.01$). These results suggest that firms should *not* delete observations from PETs users even though some of it is tainted. It seems that the amount of data is more important than the quality of data, at least in this case.

2.6 Conclusions

With increasing privacy concerns and prevalent adoption of end-user PETs by consumers, it has become important for firms whose value creation relies heavily on the mining of consumer data to understand the impact of such technologies on their analytics capabilities and performance. In this study, we seek to better understand *whether*, *how* and *when* end-user PETs affect firms' analytics capabilities and performance.

Toward this end, this study conducts a comprehensive landscape review of end-user PETs both from academic research and from technologies available in practice. New technologies are constantly emerging (e.g., differential privacy) which might provide some valuable implications and unique perspective into our research framework. The development of personal data stores (e.g., the hub-of-all-thing) are still at academic research project stages and are still far from commercial deployment. Even though there might be a new categories of end-user PETs outside of the six categories we identify, we believe that ultimately, the nature of the firm's data problem induced by end-user PETs will fundamentally relate to missing values and

[10] Here, we are assuming that firms are able to detect which consumers are users of PETs but cannot distinguish which observation is manipulated by the PETs since the PETs may not manipulate all data due to variations in protection intensity.

measurement errors in different aspects of the firm's data (i.e., entity, attributes and/or relationships).

More importantly, we abstract from our review a theoretical framework of end-user PETs that articulates the types of data challenges induced by different types of end-user PETs. Our framework can not only aptly classify end-user PETs that are in current existence but also serves as a useful tool to anticipate emerging and new future end-user PETs. The framework allows us to make sense of how each type of end-user PETs might adversely affect firms' analytics capabilities and performance via the degradation of the organizational data.

Our study also proposes an analytical approach to quantify the impact of end-user PETs on firms analytics performance and illustrate the value of our theoretical framework by applying it to the analysis of the impact of end-user PETs on product recommendation performance. This analytical methodology can easily be adapted to study the impact of other types of end-user PETs and other analytics use cases that involve consumer trace data (e.g., market basket analysis, customer segmentation, etc.).

Our findings bring to light several potentially significant challenges for firms to deal with the increasing adoption of end-user PETs. As an overall general implication, it is important for firms to reduce the adoption of end-user PETs by their consumers in order to collect as much and as high-quality consumer data as possible. In particular, at least with the product recommendation use case that we study, firms do not need to be too concerned when the adoption rate and protection intensity are relatively low. However, if the adoption rate and protection intensity are suspected to be high, firms should take actions to maintain their analytics performance. Moreover, firms should pay careful attention to their heavy users who contribute the lion's share of observations. We also note that seemingly effective response strategies, such as identifying PETs users and deleting their observations in the training of analytics models, may actually be counter-productive and lead to poorer performance.

Beyond the product recommendation use case that we study, our study opens up promising directions for future research. Although this study has only investigated the impact of PETs adoption (adoption rate and pattern) and protection characteristics (protection mechanism and intensity) on firms' analytics performance in the product recommendation use case, future studies can investigate how other such factors affect the accuracy of prediction and classification in machine learning models (e.g. support vector machines (SVM), decision tree, Naïve Bayes, neural network, etc.). Other relevant business analytics contexts, such as other recommendation systems (e.g. matrix factorization), market basket analysis, purchase predictions, etc. could also provide useful practical implications for firms.

Chapter 3

Economics of PDPs

3.1 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 great incentives to carefully engineer the privacy infrastructures (i.e, the consent interface) 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 patterns (PDPs) refer 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, with increasing privacy regulations, PDP practices are becoming more ubiquitous in a variety of contexts. Nouwens et al.

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

(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).

The focus of the early literature privacy dark pattern has been to understand its descriptive aspects, namely, to define and classify privacy dark patterns via taxonomies (Bösch et al. 2016, Mathur et al. 2021). Subsequently, the literature established 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 investigated the effectiveness of PDP either from a descriptive paradigm (Frobrukerrådet 2018, Mathur et al. 2021) or using online survey-based experiments (Nouwens et al. 2020, Luguri and Strahilevitz 2021). 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 somewhat 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 could 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 PDPs (i.e., how they will respond when recognizing the existence of PDPs). 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 uses. For instance, the Commission Nationale de L'Informatique et des Libertés (CNIL) in France shed light on the necessary control of the 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, in this study, we also investigate *whether market force are sufficient to keep PDP practices at low levels* and *what is the optimal regulation on PDP practices.*

In this study, we develop a game-theory model of privacy dark patterns (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 incentive to not utilize any privacy dark pattern practices when users' privacy cost is high and the ratio of privacy concern and the reduced search cost of opt-in is either too high or too low. This could be attributed to the fact that the *market shrink 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 essay 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.

3.2 Related Literature

The main purpose of our study is to examine the economic implications of privacy dark patterns. Firstly, privacy dark pattern is one type of dark patterns. Secondly, it influences consumers' privacy protection behaviors. Thirdly, a seller will utilize disclosed 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.

3.2.1 Dark Patterns

The stream of literature that is closest to our work is the one on dark patterns. The 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 pattern 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

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

et al. (2019) found 15 types dark patterns within 7 broader categories, namely, *sneaking*, *urgency*, *misdirection*, *social proof*, *scarcity*, *obstruction*, *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.) (Luguri and Strahilevitz 2021, Di Geronimo et al. 2020, 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 rate 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 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 the 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 patterns: 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.

3.2.2 Privacy Protection

The economics of privacy has been extensively documented in the literature. Acquisti et al. (2016) provided a comprehensive review. In this section, we briefly summarize those recent and related works after Acquisti et al. (2016) from three perspectives.

The first strand of the literature examines the incentives for a digital business to collect and protect users' personal information, in other words, data collector's self-regulation practices. In their seminal work, Casadesus-Masanell and Hervas-Drane (2015) proposed that increasing the level of user information disclosure decreases users' willing to pay and provide personal information which drives firms to maintain a certain level of privacy protection. In addition, they showed that competition intensifies the level of privacy protection. Digital platforms decide their optimal privacy strategy (e.g., full disclose vs. no disclose (De Corniere and De Nijs 2016), level of targeting (Gal-Or et al. 2018), the amount of data collected (Dimakopoulos and Sudaric 2018, Fainmesser et al. 2023), etc.) by balancing the benefits (e.g., higher demand by reducing privacy concerns or search costs for consumers) and costs (e.g., lower discrimination power which leads to lower price) from providing privacy protection (i.e., by reducing data collection and usage). Due to the two-sided nature of the market faced by digital platforms, their privacy protection strategies often depend on their business model (Fainmesser et al. 2023, Gopal et al. 2018), the extent of network effects Gopal et al. (2018), Dimakopoulos and Sudaric (2018), and consumer homing behaviors (Gopal et al. 2018).

The second strand of the literature investigates the economic implications of privacy regulation. As Acquisti et al. (2016, pp. 481) called for more research on "the specific features of regulation (and their differential effects on economics outcomes), rather than on simpler binary models contrasting regulation with its absence", especially, after the GDPR, which serves as a benchmark privacy regulation, came into effect in 2018, several analytical modeling studies have conducted welfare analysis of specific privacy policies. Gopal et al. (2020) showed that banning third-parties (i.e., full privacy protection) makes consumers worse off and website better off while consent-based policies increase consumer surplus and decrease website profit. Argenziano and Bonatti (2020) studied a set of privacy principles, namely, transparency, consent, no discrimination and direct payments for consent. They showed that the consent privacy requirement benefits consumers while mandatory transparency hurts consumers and no discrimination could make consumer either better or worse off. Lam and Liu (2020) found that the privacy policy relating to data portability can induce both a "switch-facilitating" effect and a "demand-expansion" effect. The presence of big data analytics and switching costs strengthen the "demand-expansion" effect which hiders switching and entry. As a more general framework, Bird and Neeman (2020) formulated privacy regulation as an exogenous restrictions on an informed firm's ability to persuade an uninformed consumer. Apart from these analytical works, there is a growing body of empirical works that shows that the introduction of privacy regulation (e.g., GDPR) will contribute to a reduction in technology venture investments (Jia et al. 2018), improvements in consumer traceability (Aridor et al. 2021), reduction in firm financial performance, especially for small companies (Chen et al. 2022), increases in market concentration in web technology services (Johnson et al. 2022, Peukert et al. 2022), a decline in websites technology vendor usage (Johnson et al. 2022).

The third strand of the literature, especially relevant to our work, explores the idea that 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 purpose Acquisti et al. (2016), we discuss below some of the more closely related recent works.

Koh et al. (2017) consider a model of a monopolist seller who chooses two separate prices, whereas consumers decide whether to opt-in or opt-out and whether to buy the 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 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 evidences (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 versus 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 implication of privacy dark patterns. 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.

3.2.3 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 (Koh et al. 2017, Ali et al.

2023, Ichihashi 2020, Dengler and Prüfer 2021). The impact highly depends on how and what consumer personal information is protected (i.e., no vs. full protection (Koh et al. 2017, Choi et al. 2020, Dengler and Prüfer 2021, Hu et al. 2022), 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 privacy dark patterns influence the impact of consumers' privacy protection and the digital business following a price discrimination strategy.

3.3 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 in his website. Since individuals are empowered 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., the interface for consenting to cookies) for 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) decision. In the following section, we will illustrate our players' (the seller, users) 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, $v \sim \mathcal{U}[0,1]$.

3.3.1 Seller Behavior

3.3.1.1 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 is 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 (Brownlee 2016, Aribarg and Schwartz 2020, Luguri and Strahilevitz 2021).

3.3.1.2 Pricing Regimes

In our model, the seller has the ability to differentiate opt-in users 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 users preference learning. Whereas, the seller cannot learn opt-out users' preference without information disclosure. Therefore, the seller can set a personalized price

$P_{in}(\hat{v})$ for the opt-in users based on what he learn from the personal information disclosed by the opt-in users (i.e., $\hat{v}$ is the predicted value of a user's actual product valuation v. It follow distribution $F(\cdot)$) and a uniform price P_{out} for the opt-out users.

3.3.1.3 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 predicted product valuation $\hat{v}$ and a uniformed price P_{out} for opt-out users. The seller's profit function is:

$$\pi\left(P_{in}(\hat{v}),\ P_{out},\ d\right) = \int P_{in}(\hat{v}) D_{in}(P_{in}(\hat{v}), P_{out}, d) dF(\hat{v}) + P_{out} D_{out}(P_{in}(\hat{v}), P_{out}, d) \tag{3.1}$$

3.3.2 Users Behaviour

3.3.2.1 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 (Koh et al. 2017, Choi et al. 2020, Dengler and Prüfer 2021, Hu et al. 2022) [3]. 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. Mathematically, it is a mapping from users' true valuation v to the signal realization (i.e., the predicted valuation) $\hat{v}$ observed by the seller. The literature has documented different types of signal structures

[3] 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.

(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) [4]. Thus, in the following analysis, we directly use the notation $P_{in}(v)$ rather than $P_{in}(\hat{v})$.

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), and marketing solicitations (Hann et al. 2008). Intrinsic privacy costs relate to the loss of autonomy and invasion of privacy rights (Chellappa and Shivendu 2007). In our model, a proportion $\alpha \in [\mathit{0}, \mathit{1}]$ of users are privacy sensitive (labeled as S users) and they will encounter a positive intrinsic privacy cost $r \in [\mathit{0}, \mathit{1}]$, 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, Koh et al. 2017, Ichihashi 2020, Hidir and Vellodi 2021). 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 $c \in [\mathit{0}, \mathit{1}]$ 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.

[4] The signal structure will directly affect the seller's pricing strategy for the opt-in users. To some extent, it might further influence the pricing strategy for opt-out users and the privacy dark pattern strategy. Therefore, we suggest that future studies should conduct a robustness check of when the seller cannot perfectly predict opt-in users' individual valuations, in other words, other signal structures. For example, choosing to opt-in will reveal the consumer's true valuation with only a certain probability or as pure noise, otherwise (Koh et al. 2017).

3.3.2.2 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 Tables 3.1 and 3.2, respectively. The value of the outside option of not-purchasing is normalized to zero.

Sensitive Users	**Buy**	**Not-Buy**
Opt-In	$v - P_{in}(v) - r$	$-r$
Opt-Out	$v - P_{out} - c - d$	$-d$

Table 3.1: Utility of a Privacy Sensitive User with Valuation v

Non-Sensitive Users	**Buy**	**Not-Buy**
Opt-In	$v - P_{in}(v)$	*0*
Opt-Out	$v - P_{out} - c - d$	$-d$

Table 3.2: Utility of a Privacy Non-Sensitive User with Valuation v

3.3.3 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" ($U_{in} = U_{out}$), 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".

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 $P_{in}(v)$ (i.e., by a small positive number ϵ) 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”.

3.3.4 Game Sequence and Solution Concept

Timing of the Game – The sequence of the game is presented in Figure 3.1. In stage 1, the seller chooses the level of privacy dark patterns (PDPs) d. In stage 2, the seller sets a uniform price P_{out} for opt-out users. After observing the PDP level and the uniform price P_{out}, users make their information disclosure decision using the expected price $\hat{P}_{in}(v)$ for opt-in users. In stage 3, after observing the signal realizations (i.e., the predicted valuation $\hat{v} = v$ for opt-in users) and updating his belief on the anonymous opt-out users' valuation distribution, the seller determines the personalized price $P_{in}(v)$ for opt-in users. Finally, in stage 4, after observing the offered price, both opt-in and opt-out users make purchase decisions and all payoffs are realized.

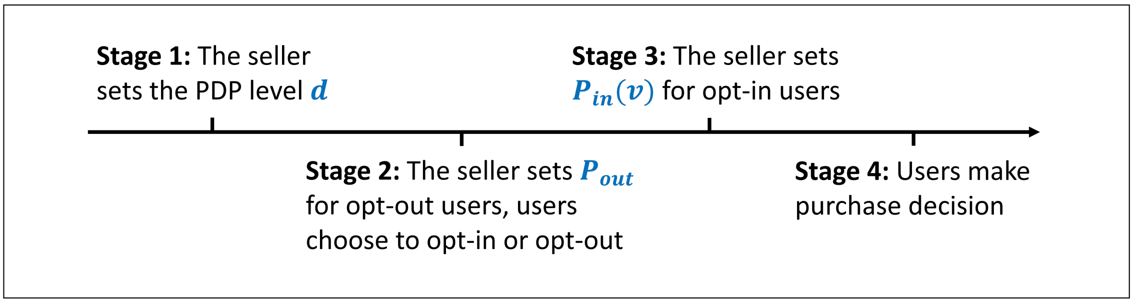

Stage 1: The seller sets the PDP level d
Stage 3: The seller sets $P_{in}(v)$ for opt-in users
Stage 2: The seller sets P_{out} for opt-out users, users choose to opt-in or opt-out
Stage 4: Users make purchase decision

Figure 3.1: Sequence of the Game

Solution Concept – Since the seller can perfectly predict opt-in users' product valuation, he will have the knowledge of 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, in the equilibrium, $\hat{P}_{in}(v) = P^*_{in}(v, \hat{P}_{in}(v))$. Thus, we have a sequential game with complete information and consequently we use the sub-game perfect equilibrium (SPB) as our solution concept. In addition, we only consider pure strategy equilibrium (see additional assumption 1 and 2). Thus, the equilibrium is a tuple of the seller's PDP level decision d^*, pricing decision

$(P^{*}_{in}(v), P^{*}_{out})$ and users information disclosure decision (i.e., opt-in or opt-out), purchase decision (buy or not buy). A summary of the notation is provided in Table 3.3.

Notation	**Description**
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
U^{S}	The utility of privacy sensitive users
U^{NS}	The utility of privacy non-sensitive users

Table 3.3: Summary of Notation

3.4 Model Analysis

3.4.1 Benchmark Case: No PDPs

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 3.1 without stage 1 where the seller sets the PDP level d. We use the backward induction approach to derive the equilibrium.

At the beginning of stage 2, the seller sets P_{out}, users observe P_{out} and form a belief about the seller's price in stage 3, denoted by $\hat{P}_{in}(v)$. Because all users have the same information about the seller, and we consider the seller using a pure strategy, all users will form the same belief $\hat{P}_{in}(v)$. Based on this belief, users make information disclosure decision (either opt-in or opt-out). Conversely, users can observe the actual price $P_{in}(v)$ when they make purchase decision in stage 4.

Stage 4: Buying – According to their utilities (see Table 3.1 and 3.2) and our additional assumptions, 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 following purchase decision). On the contrary, search cost c only incur 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. A user v will buy the product if:

$$\begin{cases} v \geq P_{in}(v), & \text{for opt-in users} \\ v \geq P_{out} + c, & \text{for opt-out users} \end{cases}$$

A personalized price $P_{in}(v)$ is offered to opt-in users while opt-out users will receive a uniform price P_{out}.

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

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

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 (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). This pricing strategy for opt-in users does not depend on users' information disclosure decision in stage 2. In other words, it does not rely on users' belief $\hat{P}_{in}(v)$ at the beginning of stage 2.

Stage 2: P_{out}, Opt-in/Opt-out – When making information disclosure decision, fully rational users will completely anticipate the above pricing strategy for opt-in users. Therefore, all users will form a belief $\hat{P}_{in}(v) = v$. Based on this belief, privacy sensitive users will know that they will receive a utility of $-r < 0$ if they choose to opt-in, while they can guarantee at least a utility of 0 if they choose to opt-out. Therefore, "Opt-in" is dominated by "Opt-out" for privacy sensitive users and they will directly choose to opt-out at stage 2. Their purchase behavior has been analyzed in the above "Stage 4: Buying" section.

For privacy non-sensitive users, they will expect a utility of 0 when they choose to opt-in since $\hat{P}_{in}(v) = v$. They will receive a utility of $v - P_{out} - c$ (i.e., buy the product) or 0 (i.e., not buy the product) if they choose to opt-out. To sum up, privacy non-sensitive users face the following options given the belief $\hat{P}_{in}(v) = v$:

$$\begin{cases} U_{in}^{NS} = 0, & \text{Opt-in in stage 2} \\ U_{out}^{NS} = max\left\{v - P_{out} - c, 0\right\} & \text{Opt-out in stage 2} \end{cases}$$

Taken together, both privacy sensitive and privacy non-sensitive users with $v \geq P_{out} + c$ will choose to opt-out and purchase the product. Privacy sensitive users with $v < P_{out} + c$ will choose to opt-out and do not purchase the product. Privacy non-sensitive users with $v < P_{out} + c$ will choose to opt-in and purchase the product. Hence the seller solves the following optimization problem in stage 2:

$$\max_{P_{out}} \pi(P_{out}) = \begin{cases} P_{out}(1 - P_{out} - c) + \dfrac{(1-\alpha)(P_{out}+c)^2}{2}, & \text{if } 0 \leq P_{out} + c < 1 \\ \dfrac{1-\alpha}{2}, & \text{if } 1 \leq P_{out} + c \end{cases}$$

This yields the optimal price P_{out} for opt-out users when there PDP is not at play (the proof is provided in the Appendix B.1):

$$P_{out}^{b*} = \begin{cases} \dfrac{1-\alpha c}{1+\alpha}, & 0 \leq c < \alpha \leq 1 \\ \overline{P}_{out}, & 0 \leq \alpha \leq c \leq 1, \text{ where } \overline{P}_{out} \geq 1 - c \end{cases} \tag{3.2}$$

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 fewer users are concern 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 fewer users are concern 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 3.2. In the equilibrium under high α (Figure 3.2(a)), all privacy sensitive users choose to opt-out; privacy non-sensitive users with low valuation choose to opt-in and purchase the product; and privacy non-sensitive users with high valuation choose to opt-out and buy the product. On the contrary, when α is low (Figure 3.2(b)), all privacy sensitive users choose to opt-out and not buy while all privacy non-sensitive users choose to opt-in and buy the product.

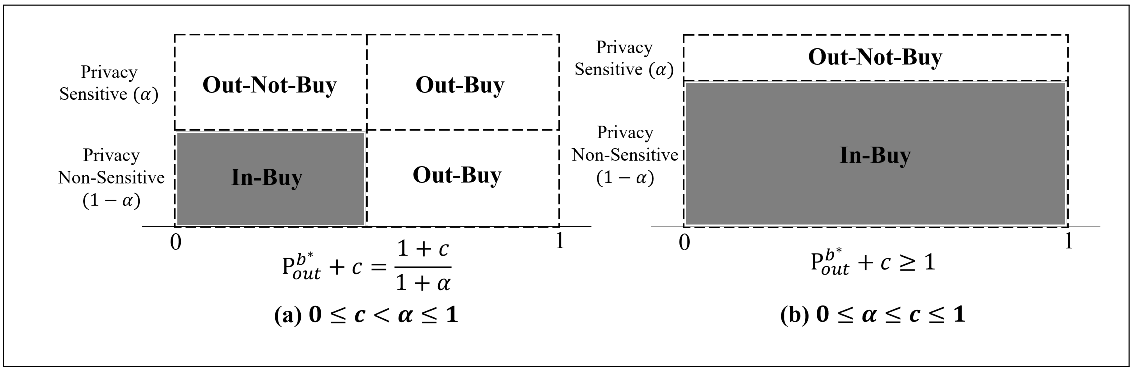

Privacy Sensitive (α)
Privacy Non-Sensitive ($1-\alpha$)
Out-Not-Buy
Out-Buy
In-Buy
Out-Buy
0
1
$P^{b^*}_{out} + c = \frac{1+c}{1+\alpha}$
(a) $0 \le c < \alpha \le 1$
Privacy Sensitive (α)
Privacy Non-Sensitive ($1-\alpha$)
Out-Not-Buy
In-Buy
0
1
$P^{b^*}_{out} + c \ge 1$
(b) $0 \le \alpha \le c \le 1$

Figure 3.2: Market Segmentation in Benchmark Equilibrium

Lemma 1. *(Benchmark). The equilibrium without PDPs is characterized as following:*

(1) ***Low privacy concern*** *($\alpha \le c$)*

- $P^{b*}_{in}(v) = v$, $P^{b*}_{out} \ge 1 - c$
- *S users choose "Opt-out and Not-buy" while NS users choose "Opt-in and Buy".*

(2) ***High privacy concern*** *($\alpha > c$)*

- $P^{b*}_{in}(v) = v$, $P^{b*}_{out} = \dfrac{1-\alpha c}{1+\alpha}$
- *High valuation users choose to "Opt-out and Buy". Low valuation S users choose to "Opt-out and Not-buy" while low valuation NS users choose to "Opt-in and Buy".*
- *The proportion of opt-in users is decreasing in privacy concern (α) but increasing in search cost (c).*
- *The seller's profit 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).*

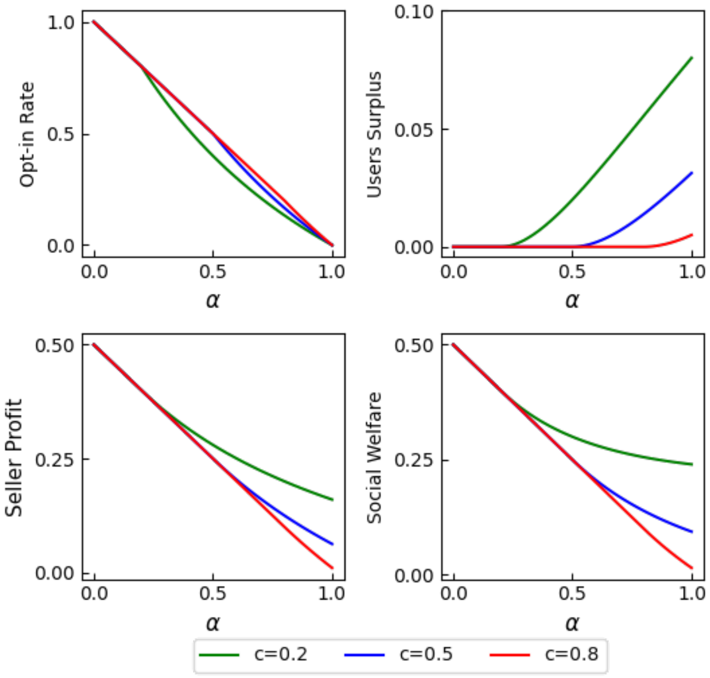


Figure 3.3: Effect of Privacy Concern (α) and Search Cost (c) in Benchmark Equilibrium

Lemma 1 is the result of the tradeoff 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 only consisted only of privacy non-sensitive (NS) users and opt-out market including 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 opt-out market, which contributes to a lower total profit (Figure 3.4(a)).

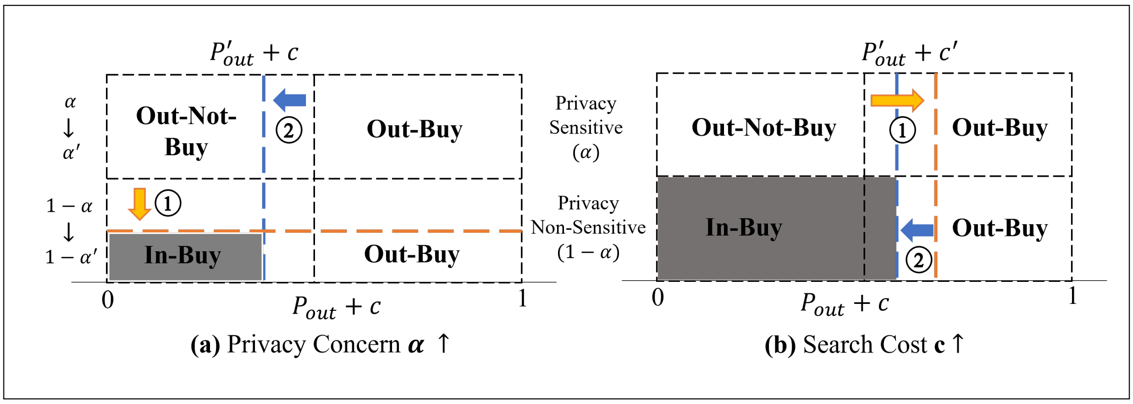


Figure 3.4: Static Comparative Analysis in Benchmark Equilibrium

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 opt-in market expansion can not compensate the loss from the shrinkage of the opt-out market. Thus, the total profit goes down (Figure 3.4(b)).

3.4.2 PDPs 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 Tables 3.1 and 3.2. The timing of game is depicted in Figure 3.1. Similarly, we use backward induction to derive the equilibrium.

Stage 4: Buying – Since the additional cost d imposed by PDP practices 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 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 $P_{in}(v)$ – Following the same logic in 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:

$$P_{in}^{n*}(v) = v \tag{3.3}$$

Stage 2: P_{out}**, Opt-in/Opt-out** – Given the pricing strategy (Equation 3.3) for opt-in users in stage 3 and the uniform price P_{out} they observe, users would like to maximize their utility by choosing to opt-in or opt-out:

$$U^{NS} = max\left\{U_{in}^{NS},\ U_{out}^{NS}\right\} = max\left\{0,\ max\left\{v - P_{out} - c - d,\ -d\right\}\right\}, \text{ for } NS \text{ users}$$
$$U^{S} = max\{U_{in}^{S},\ U_{out}^{S}\} = max\left\{-r,\ max\left\{v - P_{out} - c - d,\ -d\right\}\right\}, \text{ for } S \text{ users}$$

As can be seen, privacy non-sensitive (NS) users will either choose "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 "Opt-out and Buy" or "Opt-out and Not-buy." It is similar to the case in benchmark case. There will be some privacy sensitive (S) users 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. Detailed mathematical proofs are available in the Appendix B.2.

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 following:*

- $P_{in}^{n*}(v) = v$, $P_{out}^{n*} \geq 1 - c - d^{n*} + r$, $d^{n*} \geq r$
- *All users choose to "Opt-in and Buy". The market is fully covered.*

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 users' 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 care about any 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 or receive any digital service.

3.4.3 PDPs 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 concern makes 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 level for the seller when users are sophisticated. Users are sophisticated such that they can recognize and negatively react to the presence of PDP designs 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 main analysis.

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

$$P_{in}^{s*}(v) = v \tag{3.4}$$

Therefore, the seller faces the following profit function given a combination of P_{out} and d:

$$\pi(P_{out},\ d) = \Big[\alpha\pi^{S}(P_{out}, d) + (1-\alpha)\pi^{NS}(P_{out}, d)\Big]\,(1-d) \tag{3.5}$$

where:

$$\pi^{NS}(P_{out},\ d) = \int_0^{min\{1,\ P_{out}+c+d\}} vdv + P_{out}\,(1 - min\{1,\ P_{out}+c+d\})$$

$$\pi^{S}(P_{out},\ d) = \begin{cases} P_{out}(1 - min\{1,\ P_{out}+c\}), & \text{if} \quad 0 \le d < r \\ \displaystyle\int_0^{min\{1,\ P_{out}+c+d-r\}} vdv + P_{out}(1 - min\{1,\ P_{out}+c+d-r\}), & \text{otherwise} \end{cases}$$

There is a tradeoff 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 expends 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.

We follow the backward induction approach to figure out the equilibrium. Detailed proof can be found in Appendix B.3.

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 following*[5]*:*

[5] where $\overline{r}_i$ depends on the combination of α and c (i.e., $\overline{r}_1$ for $(\alpha,\ c)$ in area I, $\overline{r}_2$ for $(\alpha,\ c)$ in area II). The specific values of $\overline{r}_i$ (i.e., $\overline{r}_1$, $\overline{r}_2$, $\overline{r}_3$, $\overline{r}_4$), x_1, and x_4 can be found in the Appendix B.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 3.4: Equilibrium with Sophisticated Users

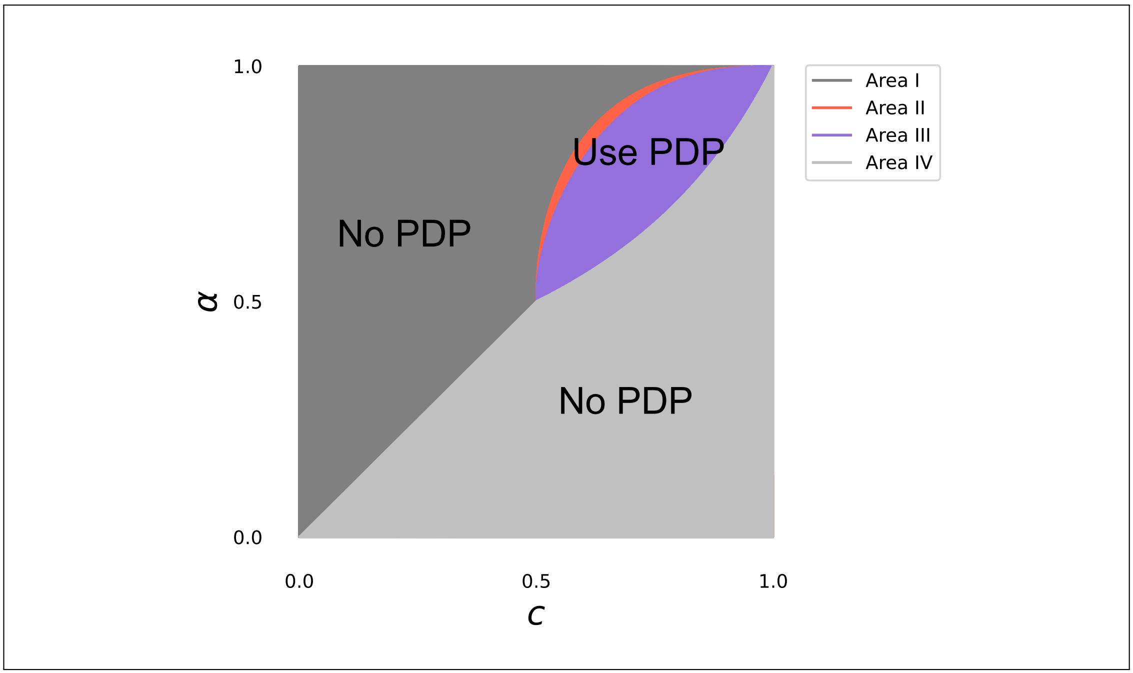


Figure 3.5: Equilibrium with Sophisticated Users Under High Privacy Cost (r)

Lemma 3 and Figure 3.5 present 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 the privacy cost r is low, similar to the naïve users case, the seller will set a high P_{out} (where $\overline{P}_{out} \geq 1 - c$) 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 (Figure 3.6(0)). 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 c is relatively low (area I), or privacy concern α is low and the search cost c is relatively high (area IV), the seller prefers ***not to utilize any privacy dark pattern design*** ($d = 0$) which is similar to the benchmark case. The market force is strong enough to incentive the seller to be privacy friendly. Nevertheless, when both the privacy concern α and search cost c is high (area II and III, the seller will choose a moderate PDP design strategy d).

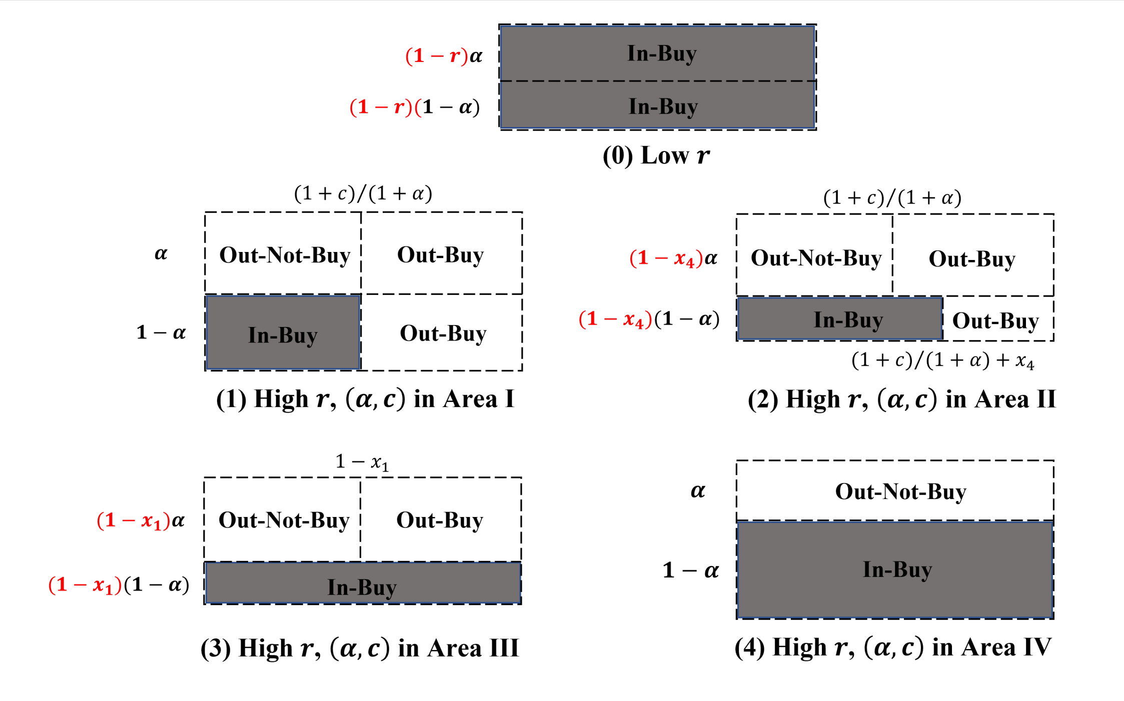


Figure 3.6: Market Segmentation in Equilibrium with Sophisticated Users

3.5 Impact of PDPs

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. The detail proof can be found in the Appendix B.5.

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

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 users' surplus. The seller is strictly better off with the presence of PDP when users are naïve. According to Figure 3.2, 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 situation, he can abandon PDP to achieve the same profit as the benchmark without PDP. Our analysis shows that, regardless of the magnitude of privacy concern (α), search cost (c) and privacy cost (r), users are weakly worse off with the presence of PDPs. Nevertheless, the change of total social welfare depends on the magnitude of privacy concern (α), search cost (c) and privacy cost (r).

3.6 Regulation on PDPs

With increasing concerns over the proliferation of privacy dark patterns, the public has recently called for regulation over PDPs (FTC 2021, CNIL 2019, EDPB 2022). It is commonly believed that PDPs should be fully prohibited as they go against users' best interest. In the previous section, our results has shown that the introduction of PDPs indeed makes users weakly worse off. However the presence of PDPs 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 through regulating over PDP practices. In stage 1, the social planner will set a PDP level d to maximize social welfare rather than the seller decides d to maximize its profit. The detailed proof can be found in Appendix B.6.

Proposition 2. *(Social Optimal PDP Level). A social welfare maximizing planner* *will choose the following PDP level* [6]*:*

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

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 $(\alpha,\ c)$. Nevertheless, the social optimal PDP level is ***non-zero*** when r is low enough. In other words, the presence of PDP practice increases social welfare when the privacy cost r is low. The reason is that setting $d = r$ will transfer 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.

3.7 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 users' surplus (CS), seller profits (π) and total social welfare (TW). According to lemma 3, we conduct static comparative analysis with respect to α, c and r (the proof is provided in the Appendix B.4).

3.7.1 Users' Surplus, Seller Profit, and Social Welfare

Consumer surplus consists of consumption utility and search cost in stage 4, privacy cost (r for S users and 0 for NS users) and additional opt-out cost d imposed by PDPs in stage 2. According to users' utility in Tables 3.1 and 3.2, a user v will receive $-r$ (for S users) or 0 (for NS users) if she chooses to opt-in and buy the product due to perfect price discrimination. If she chooses to opt-out and buy (or not buy), she will receive utility $v - P_{out} - c - d$ (or $-d$) (for both S and NS users). Figure 3.6 presents users segmentation in equilibrium under different combinations of α, c, and r. We derive consumers surplus and profits for each case in Appendix B.4.

[6] The specific values of $\overline{r}$ depend on the combination of $(\alpha,\ c)$ which can be found in the Appendix B.6.

3.7.2 Comparative Statics for Privacy Concern 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, profits, and social welfare (ceteris paribus)* [7]*:*

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 3.5: Effect of Users' Privacy Concern α

Lemma 4 shows that the impacts of α on users' surplus, profit and total social welfare depend on r and c. When the privacy cost r is low (Figure 3.6(0)), 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: $(P^{s*}_{out}, d^{s*}) = (\overline{P_{out}}, r)$ 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 users' surplus and social welfare depend on c. For (α, c) in area I (Figure 3.6(1)), the optimal PDP level is 0 and the price for opt-out users is decreasing in α. The positive users' 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, users' surplus is increasing in α. Increasing α makes more privacy sensitive users uncovered by the market which contributes to a lower social welfare.

[7] where $\overline{r}_i$ depends on the combination of $(\alpha,\ c)$ (i.e., $\overline{r}_1$ for $(\alpha,\ c)$ in area I, $\overline{r}_2$ for $(\alpha,\ c)$ in area II). The specific values of $\overline{r}_i$ (i.e., $\overline{r}_1$, $\overline{r}_2$, $\overline{r}_3$, $\overline{r}_4$) can be found in the Appendix B.4.

Nevertheless, for (α, c) in area II, both users' 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 (Figure 3.6(4)), 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 users' surplus. Thus, users' surplus is independent of α while social welfare is decreasing in α since the seller's profit is decreasing in α.

3.7.3 Comparative Statics for Search Cost c

Lemma 5. *(Effects of Search Cost c). Raising the search cost c has the following effects on users' surplus, seller's profits, and social welfare (ceteris paribus)* [8]*:*

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

Table 3.6: Effect of Search Cost c

Lemma 5 shows that when the privacy cost r is low (Figure 3.6(0)), or high and (α, c) is in area IV (Figure 3.6(4)), the users' surplus, seller's profits and social welfare are independent on search cost c. Nevertheless, when the privacy cost r is high and (α, c) is in area I or II, users' surplus, seller's 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's profit is decreasing while both users' surplus and social welfare are increasing in search cost c.

[8] where $\overline{r}_i$ depends on the combination of $(\alpha,\ c)$ (i.e., $\overline{r}_1$ for $(\alpha,\ c)$ in area I, $\overline{r}_2$ for $(\alpha,\ c)$ in area II). The specific values of $\overline{r}_i$ (i.e., $\overline{r}_1$, $\overline{r}_2$, $\overline{r}_3$, $\overline{r}_4$) can be found in the Appendix B.4.

3.7.4 Comparative Statics for Privacy Cost r

Lemma 6. *(Effects of Privacy Cost r). Raising the privacy cost r has the following effects on users' surplus, seller's profits, and social welfare (ceteris paribus)* [9]*:*

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 3.7: Effect of Privacy Cost r

Lemma 6 shows that when the privacy cost r is low, users' surplus, seller's profits and social welfare are decreasing in r. Nevertheless, when it is high enough, users' surplus, profits and social welfare are independent on r.

3.8 Extensions

3.8.1 Different PDP Sensitivity λ

For simplification, we have assumed that the PDP sensitivity $\lambda = 1$ in the above analysis. However, it is easy to imagine that the magnitude of λ influences the seller's pricing and PDP strategies. For instance, when λ is high enough, it is optimal for the seller not to embrace PDP practices. On the contrary, the seller prefers to aggressively adopt PDP practices if λ is quite low. Therefore, in this section, we extend our analysis for different value of λ. Since the majority of our variables are normalized between 0 and 1, we conduct robustness check for $\lambda = 0.5$ and $\lambda = 2$. The detailed proof can be found in the Appendix B.7.

3.8.1.1 $\lambda = 0.5$

Our analyses show that when $\lambda = 0.5$, the equilibrium is characterized as following [10]:

[9] where $\overline{r}_i$ depends on the combination of $(\alpha,\ c)$ (i.e., $\overline{r}_1$ for $(\alpha,\ c)$ in area I, $\overline{r}_2$ for $(\alpha,\ c)$ in area II). The specific values of $\overline{r}_i$ (i.e., $\overline{r}_1$, $\overline{r}_2$, $\overline{r}_3$, $\overline{r}_4$) can be found in the Appendix B.4.

[10] The specific values of $\overline{r}_i^{05}$ depend on the combination of $(\alpha,\ c)$ which can be found in the Appendix B.7.1

r	$(\alpha,\ c)$	P_{out}^{s*}	d^{s*}	P_{in}^{s*}
Low $r \in [0,\ \overline{r}_i^{05}]$	All Areas	$\geq 1-c$	r (Use PDP)	v
High $r \in (\overline{r}_i^{05},\ 1]$	Area I	$\dfrac{1-\alpha c}{1+\alpha}$	0 (No PDP)	
	Area II	$1-c-x_1$	x_1 (Use PDP)	
	Area III	$\geq 1-c$	0 (No PDP)	

Table 3.8: Equilibrium with Sophisticated Users for $\lambda = 0.5$

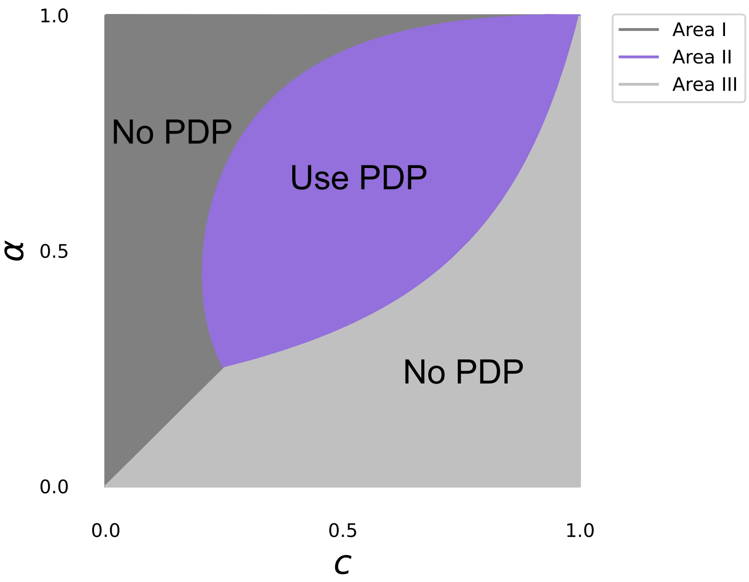


Figure 3.7: Equilibrium with Sophisticated Users Under Low PDP Sensitivity ($\lambda = 0.5$)

As can be seen, our main results are still consistent when $\lambda = 0.5$. The seller still sets a high level of PDP ($d^{s*} = r$) when the privacy cost is low ($r \leq \overline{r}_i^{05}$). When privacy cost is low and the ratio of privacy concern α and reduced search cost c is either too high (area I) or too low (area III), the seller has incentive to not utilize PDP practices. Similarly, the optimal PDP level will be moderate if the privacy cost is low and $(\alpha,\ c)$ in area II. Nevertheless, the decision boundaries slightly change. When users are less sensitive to PDP designs (low λ), the seller is more likely to embrace PDP practices (a bigger area II, a higher cutoff value $\overline{r}$, such as, a higher r_1, r_2, and r_3).

3.8.1.2 $\lambda = 2$

Our analyses show that when $\lambda = 2$, the equilibrium is characterized as following [11]:

r	$(\alpha,\ c)$	P_{out}^{s*}	d^{s*}	P_{in}^{s*}
Low $r \in [0,\ \overline{r}_i^2]$	All areas	$\geq 1 - c$	r (Use PDP)	v
High $r \in (\overline{r}_i^2,\ 1]$	Area I	$\dfrac{1-\alpha c}{1+\alpha}$	0 (No PDP)	
	Area II	$\geq 1 - c$	0 (No PDP)	

Table 3.9: Equilibrium with Sophisticated Users for $\lambda = 2$

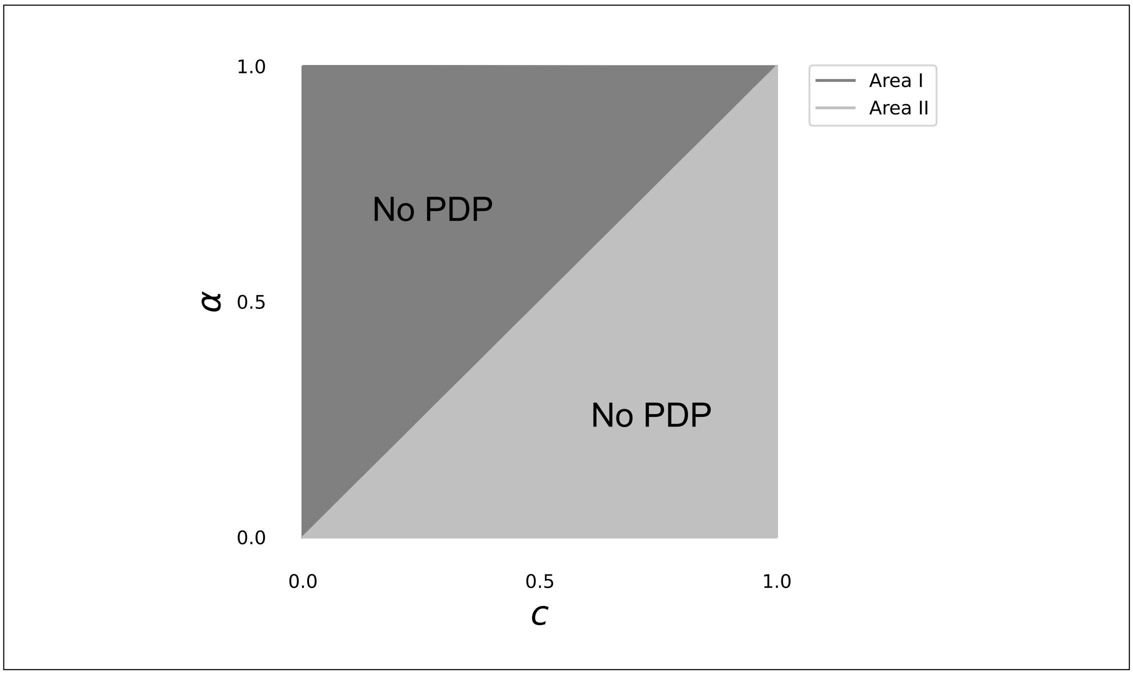


Figure 3.8: Equilibrium with Sophisticated Users Under High PDP Sensitivity ($\lambda = 2$)

[11] For $(\alpha,\ c)$ in area I, $\overline{r}_1^2 = \dfrac{\alpha - c^2 + 2\alpha c}{2(1+\alpha)}$; for $(\alpha,\ c)$ in area II, $\overline{r}_2^2 = \dfrac{\alpha}{2}$

As can be seen, when PDP sensitivity λ and privacy cost r are high enough, the equilibrium is the same as our benchmark where there is no PDP. In other words, when users are heavily sensitive to PDP designs and users are heavily privacy sensitive, it is optimal for the seller to abandon PDP practices all together. On the contrary, when the privacy cost is low enough, the seller will set a high PDP regardless of the high PDP sensitivity.

3.9 Conclusion

In this essay, 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 ration of privacy concern and reduced search cost is either too high or too low. In other words, the market force could be strong enough to achieve a no PDP design world. However, in most cases, the seller will adopt some levels 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}.

Chapter 4

Conclusion

The main goal of this dissertation is to understand the roles individuals and firms play in the process of privacy protection. In particular, the first essay examines the impact of end-user privacy enhancing technologies (PETs) adopted by individuals on firms analytical capabilities. The second essay investigates the economic implications of privacy dark pattern (PDP) practices employed by firms to influence individuals' personal information disclosure behaviour.

The first essay conducts a comprehensive review of end-user PETs from both academic and practical perspectives. We propose a data-oriented framework to qualitatively argue that end-user PETs induce measurement error and/or missing values with regards to attributes, entities and relationships in firms' customer data. Apart from this qualitative framework, we also propose a value-oriented framework through which firms can use to quantify the impact of end-user PETs on their value creation process. We illustrate the value of this framework by applying it in a simulation study to quantify the impact of end-user PETs on firms in the context of product recommendations. The simulation results show that the presence of end-user PETs decreases the performance of recommendation algorithms. This impact depends on PET characteristics (i.e., protection intensity and protection mechanism) and consumer adoption characteristics (i.e., adoption rate and adoption pattern). In addition, our results find the spillover effect of end-user PET adoption. In other words, recommendation accuracy for those individuals who do not adopt PETs also decreases. Finally, we show that the simple "deleting all" strategy (i.e., simply removing the data from individuals that have adopted PETs from the analysis) could even further deteriorate recommendation performance.

The first essay extends our knowledge of the impact of end-user PETs on firm from a data perspective. The data- and value-oriented frameworks provide actionable guidelines to utilize data corrupted by end-user PETs. In particular, when conducting business analytics using consumer data, the firm should carefully identify whether their consumers have adopted end-user PETs and determine what kind of PETs are adopted. Our data-oriented framework allows us to map how the use of different PETs will alter the firm's data. Moreover, our value-oriented framework informs firms about how to utilize appropriate statistical techniques to handle the data integrity challenges induced by end-user PETs.

The second essay build a game-theoretic model consisting of a monopolistic seller and many heterogeneous users to examine the economic implication of privacy dark patterns. The seller faces a trade-off when he decides the PDP level. On the one hand, increasing the PDP level could make users more likely to opt-in which empowers information collection and learning of users preference. On the other hand, it could hurt the seller's trustworthiness. Our results show that the presence of PDP practices makes users weakly worse off while makes the seller weakly better off. Nevertheless, the seller has incentive to not utilize any PDP practices when the users' privacy cost is high enough and the ratio of privacy concern and the reduced search cost for opt-in is either too high or too low. Even though the advent of PDPs go against users interest, a social welfare maximizing social planner will still allow a non-zero (even high) PDP level when the privacy cost is low enough since the gain from covering more users dominate the loss from privacy cost.

The second essay suggests that it is not always a good strategy for the digital business to employ PDP designs. Even though it could deceive naïve users and induce them to share their personal information, it might also hurt the digital business's credibility and contribute to negative reactions among sophisticated users. The optimal PDP strategy will depend on users' privacy concerns, privacy cost and reduced search cost for opt-in. We also provide policy implications for PDP regulation. When the privacy cost is low enough, the presence of privacy dark pattern could increase total social welfare. Nevertheless, a consumer surplus maximizing social planner should ban PDP practices.

Take together, privacy protection is a complex phenomenon where stakeholders take actions to protect their best interests and affect other players' actions. Individuals self-protection behaviors (e.g., adoption and use of end-user PETs) significantly influence firms business analytics capabilities which disproportionately affect PET adopters and PET non-adopters. Strategic firms' actions (in our study, privacy dark patterns (PDPs)) can weaken the individuals privacy protection. This dissertation offers valuable insights into this complex and emerging phenomenon.

Bibliography

Abdalla M, Bellare M, Catalano D, Kiltz E, Kohno T, Lange T, Malone-Lee J, Neven G, Paillier P, Shi H (2005) Searchable Encryption Revisited: Consistency Properties, Relation to Anonymous IBE, and Extensions. Shoup V, ed., *Proceedings of the Annual International Cryptology Conference*, 205–222 (Berlin, Heidelberg: Springer).

Ackerman MS (2004) Privacy in Pervasive Environments: Next Generation Labeling Protocols. *Personal and Ubiquitous Computing* 8(6):430–439.

Acquisti A, Brandimarte L, Loewenstein G (2015) Privacy and Human Behavior in the Age of Information. *Science* 347(6221):509–514.

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

Adomavicius G, Zhang J (2012) Impact of Data Characteristics on Recommender Systems Performance. *ACM Transactions on Management Information Systems* 3(1):1–17.

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

Anderson SP, Gans JS (2011) Platform Siphoning: Ad-avoidance and Media Content. *American Economic Journal: Microeconomics* 3(4):1–34.

Angulo J, Fischer-Hübner S, Pulls T, Wästlund E (2015) Usable Transparency with the Data Track: A Tool for Visualizing Data Disclosures. *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (Extended Abstracts)*, 1803–1808 (Seou, Korea).

Argenziano R, Bonatti A (2020) Information Revelation and Privacy Protection, *Available At: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3688155.*

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

Aridor G, Che YK, Salz T (2021) The Effect of Privacy Regulation on the Data Industry: Empirical Evidence from GDPR. *Proceedings of the 22nd ACM Conference on Economics and Computation*, 93–94.

Armknecht F, Boyd C, Carr C, Gjosteen K, Jaschke A, Reuter CA, Strand M (2015) A Guide to Fully Homomorphic Encryption. *Cryptol 2015*, 1–35 (International Association for Cryptologic Research), *Avaiable At: https://eprint.iacr.org/2015/1192*.

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

Aseri M, Dawande M, Janakiraman G, Mookerjee VS (2020) Ad-blockers: A Blessing or a Curse? *Information Systems Research* 31(2):627–646.

Auxier B, Rainie L, Anderson M, Perrin A, Kumar M, Turner E (2019) Americans and Privacy: Concerned, Confused, and Feeling a Lack of Control Over Their Personal Information. Technical report, Pew Research Center, *Available At: https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/*.

Bajari P, Chernozhukov V, Hortaçsu A, Suzuki J (2019) The Impact of Big Data on Firm Performance: An Empirical Investigation. *AEA Papers and Proceedings*, volume 109, 33–37 (American Economic Association).

Bansal G (2017) Distinguishing Between Privacy and Security Concerns: An Empirical Examination and Scale Validation. *Journal of Computer Information Systems* 57(4):330–343.

Barreno M, Nelson B, Sears R, Joseph AD, Tygar JD (2006) Can Machine Learning Be Secure? *Proceedings of the 2006 ACM Symposium on Information, Computer and Communications Security*, 16–25.

Bélanger F, Crossler RE (2011) Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarterly* 35(4):1017–1041.

Bennett CJ, Raab CD (2020) Revisiting the Governance of Privacy: Contemporary Policy Instruments in Global Perspective. *Regulation and Governance* 14(3):447–464.

Bird D, Neeman Z (2020) What Should a Firm Know? Protecting Consumers' Privacy Rents. *American Economic Journal: Microeconomics* 14(4):257–295.

Biryukov A, Pustogarov I, Thill F, Weinmann RP (2014) Content and Popularity Analysis of TOR Hidden Services. *Proceedings of the 2014 IEEE 34th International Conference on Distributed Computing Systems Workshops (ICDCSW)*, 188–193 (Washington, DC).

Blockthrough (2021) The Rise of Consent-based Advertising. Technical report, Blockthrough, *Available At: https://f.hubspotusercontent10.net/hubfs/4682915/Adblock%20Reports/2021%20PageFair%20Adblock%20Report.pdf*.

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

Bound J, Brown C, Mathiowetz N (2001) Measurement Error in Survey Data. Heckman JJ, Leamer E, eds., *Handbook of Econometrics*, volume 5, 3705–3843 (Elsevier).

boyd d, Hargittai E (2010) Facebook Privacy Settings: Who Cares? *First Monday* 15(8).

Brandimarte L, Acquisti A, Loewenstein G (2013) Misplaced Confidences: Privacy and the Control Paradox. *Social Psychological and Personality Science* 4(3):340–347.

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

Buonaccorsi JP (2010) *Measurement Error: Models, Methods, and Applications* (Boca Raton, Florida, United States: CRC Press, Taylor & Francis Group).

Burgess M (2022) How GDPR Is Failing. WIRED, *Available At: https://www.wired.com/story/gdpr-2022/*.

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

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

Chaum D (1988) The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability. *Journal of Cryptology* 1(1):65–75.

Chaum DL (1981) Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. *Communications of the ACM* 24(2):84–90.

Chellappa RK, 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):193–225.

Chen C, Frey CB, Presidente G (2022) Privacy Regulation and Firm Performance: Estimating the GDPR Effect Globally, *Available At: https://www.oxfordmartin.ox.ac.uk/downloads/Privacy-Regulation-and-Firm-Performance-Giorgio-WP-Upload-2022-1.pdf*.

Chen Y, Liu Q (2021) Signaling Through Advertising When Ad Can Be Blocked. *Marketing Science* 41(1):166–187.

Choi WJ, Jerath K, Sarvary M (2020) Advertising and Price Competition Under Consumer Data Privacy Choices, *Available At: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3708273*.

Clarke R (2009) Business Cases for Privacy-enhancing Technologies. *Electronic Business: Concepts, Methodologies, Tools, and Applications*, 895–909 (IGI Global).

CNIL (2019) Shaping Choices in the Digital World. *Available At: https://linc.cnil.fr/sites/default/files/atoms/files/cnil_ip_report_06_shaping_choices_in_the_digital_world.pdf*.

Codd E (1970) A Relational Model of Data for Large Shared Data Banks. *Communications of the ACM* 13(6):377–387.

Cranor LF (2003) P3P: Making Privacy Policies More Useful. *IEEE Security and Privacy* 1(6):50–55.

Danezis G, Gürses S (2010) A Critical Review of 10 Years of Privacy Technology. *Proceedings of Surveillance Cultures: A Global Surveillance Society?*, 1–16.

De Corniere A, De Nijs R (2016) Online Advertising and Privacy. *The RAND Journal of Economics* 47(1):48–72.

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

Despotakis S, Ravi R, Srinivasan K (2021) The Beneficial Effects of Ad Blockers. *Management Science* 67(4):2096–2125.

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

Diaz C, Gürses S (2012) Understanding the Landscape of Privacy Technologies. *Proceedings of the Information Security Summit*, 58–63.

Dimakopoulos PD, Sudaric S (2018) Privacy and Platform Competition. *International Journal of Industrial Organization* 61:686–713.

Dincelli E, Goel S, Warkentin M (2017) Understanding Nuances of Privacy and Security in the Context of Information Systems. *Proceedings of Americas Conference on Information Systems*, 1–5 (Boston, MA).

Division TA (2017) Privacy Enhancing Technologies – A Review of Tools and Techniques. Technical report, Office of the Privacy Commissioner of Canada, *Available At: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2017/pet_201711/*.

Dwork C (2008) Differential Privacy : A Survey of Results. Agrawal M, Du DZ, Duan Z, Li A, eds., *Proceedings of 5th International Conference on Theory and Applications of Models of Computation*, 1–19 (Berlin Heidelberg: Springer-Verlag).

EDPB (2022) Guidelines 3/2022 on Dark Patterns in Social Media Platform Interfaces: How to Recognise and Avoid Them. *Available At: https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf*.

Fainmesser IP, Galeotti A, Momot R (2023) Digital Privacy. *Management Science* 69(6):3157–3173.

Fischer-Hbner S, Berthold S (2017) Privacy-Enhancing Technologies. Vacca JR, ed., *Computer and Information Security Handbook*, 759–778 (Elsevier).

Fritsch L (2007) State of the Art of Privacy-enhancing Technology (PET). Technical report, Norsk Regnesentral, Norwegain Computing Center, *Available*

At: *file:///C:/Users/e0212241/Downloads/Fritsch_-_State_of_the_Art_of_Privacy-enhancing_Technology.pdf*.

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

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*.

Gal-Or E, Gal-Or R, Penmetsa N (2018) The Role of User Privacy Concerns in Shaping Competition among Platforms. *Information Systems Research* 29(3):698–722.

Ghose A (2017) When Push Comes to Shove, How Quickly Will You Give Up Your Data for Convenience? Quartz (qz.com), *Available At: https://qz.com/973578/data-privacy-doesnt-seem-to-be-a-concern-for-mobile-users-willing-to-swap-it-for-convenience/*.

Goh KY, Hui KL, Png IP (2015) Privacy and Marketing Externalities: Evidence from Do Not Call. *Management Science* 61(12):2982–3000.

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

Gopal RD, Hidaji H, Kutlu SN, Patterson RA, Yaraghi N (2020) Economics of Data Protection Polices. *Proceedings of International Conference on Information Systems*, 1–15.

Gopal RD, Hidaji H, Patterson RA, Rolland E, Zhdanov D (2018) How Much to Share with Third Parties? User Privacy Concerns and Website Dilemmas. *MIS Quarterly* 42(1):143–164.

Grčar M, Mladenič D, Fortuna B, Grobelnik M (2005) Data Sparsity Issues in the Collaborative Filtering Framework. Nasraoui O, Zaïane O, Spiliopoulou M, Mobasher B, Masand B, Yu P, eds., *Proceedings of the 7th International Workshop on Knowledge Discovery on the Web (WebKDD 2005)*, 58–76 (Berlin, Heidelberg: Spinger).

Gupta M, George JF (2016) Toward the Development of a Big Data Analytics Capability. *Information & Management* 53(8):627–646.

Hann IH, Hui KL, Lee SYT, Png IP (2008) Consumer Privacy and Marketing Avoidance: A Static Model. *Management Science* 54(6):1094–1103.

Harper FM, Konstan JA (2015) The MovieLens Datasets: History and Context. *ACM Transactions on Interactive Intelligent Systems* 5(4):1–19.

Heurix J, Zimmermann P, Neubauer T, Fenz S (2015) A Taxonomy for Privacy Enhancing Technologies. *Computers and Security* 53:1–17.

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

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

Huang L, Joseph AD, Nelson B, Rubinstein BI, Tygar JD (2011) Adversarial Machine Learning. *Proceedings of the 4th ACM workshop on Security and artificial intelligence*, 43–58.

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

Ichihashi S (2023) Dynamic Privacy Choices. *American Economic Journal: Microeconomics* 15(2):1–40.

Janic M, Wijbenga JP, Veugen T (2013) Transparency Enhancing Tools (TETs): An Overview. *Proceedings of the 2013 Third Workshop on Socio-Technical Aspects in Security and Trust*, 18–25 (Washington, DC).

Jia J, Jin GZ, Wagman L (2018) The Short-run Effects of GDPR on Technology Venture Investment, *Available At: https://www.nber.org/papers/w25248*.

Johnson G, Shriver S, Goldberg S (2022) Privacy & Market Concentration: Intended & Unintended Consequences of the GDPR, *Available At: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3477686*.

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

Kurakin A, Goodfellow I, Bengio S (2016) Adversarial Machine Learning at Scale. *arXiv preprint arXiv:1611.01236* .

Lam WMW, Liu X (2020) Does Data Portability Facilitate Entry? *International Journal of Industrial Organization* 69:102564.

Li N, Li T, Venkatasubramanian S (2007) t-Closeness: Privacy Beyond k-Anonymity and l-Diversity. *Proceedings of the 2007 IEEE 23rd International Conference on Data Engineering*, 106–115.

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

Little RJ, Rubin DB (2019) *Statistical Analysis with Missing Data* (Hoboken, NJ: John Wiley & Sons).

Liu B, Andersen MS, Schaub F, Almuhimedi H, Zhang S, Sadeh N, Acquisti A, Agarwal Y, Liu B, Andersen MS, Schaub F, Almuhimedi H, Zhang S, Sadeh N, Acquisti A, Agarwal Y (2016) Follow My Recommendations: A Personalized Privacy Assistant for Mobile App Permissions. *Twelfth Symposium on Usable Privacy and Security*, 27–41.

London Economics (2010) Study on the Economic Benefits of Privacy-enhancing Technologies (PETs). Technical report, The European Commission DG Justice, Freedom and Security, *Available At: https://op.europa.eu/en/publication-detail/-/publication/a2b75ceb-ada3-4e53-866f-7193f7270a85*.

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

Machanavajjhala A, Kifer D, Gehrke J, Venkitasubramaniam M (2007) l-Diversity: Privacy Beyond k-Anonymity. *ACM Transactions on Knowledge Discovery from Data* 1(1):1–52.

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

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

McAfee A, Brynjolfsson E (2012) Big Data: The Management Revolution. *Harvard Business Review* 90(10):60–68.

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

Peukert C, Bechtold S, Batikas M, Kretschmer T (2022) Regulatory Spillovers and Data Governance: Evidence from the GDPR. *Marketing Science* 41(4):746–768.

Pfitzmann A, Waidner M (1987) Networks Without User Observability. *Computers & Security* 6(2):158–166.

Ray A, Ghasemkhani H, Kannan KN (2017) Extortionists or Digital Age Robin Hoods?, *Available At: https://ssrn.com/abstract=2991805*.

Reed MG, Syverson PF, Goldschlag DM (1998) Anonymous Connections and Onion Routing. *IEEE Journal on Selected Areas in Communications* 16(4):482–494.

Rubin DB (1976) Inference and Missing Data. *Biometrika* 63(3):581–592.

Shen Y, Pearson S (2011) Privacy Enhancing Technologies: A Review. Technical report, Hewlett-Packard Development Company, *Available At: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.377.2136&rep=rep1&type=pdf*.

Shiller B, Waldfogel J, Ryan J (2018) The Effect of Ad Blocking on Website Traffic and Quality. *RAND Journal of Economics* 49(1):43–63.

Smith B, Linden G (2017) Two Decades of Recommender Systems at Amazon.com. *IEEE Internet Computing* 21(3):12–18.

Smith JH, Dinev T, Xu H (2011) Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly* 35(4):989–1015.

Solove DJ (2012) Introduction: Privacy Self-management and the Consent Dilemma. *Harvard Law Review* 126(7):1880–1903.

Sweeney L (2002) k-Anonymity: A Model for Protecting Privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems* 10(5):158–166.

Tucker C (2022) The Economics of Privacy: An Agenda. *NBER Chapters* .

van Blarkom GW, Borking JJ, Verhaar P (2003) PET. van Blarkom G, Borking JJ, Olk J, eds., *Handbook of Privacy and Privacy-Enhancing Technologies: The Case of Intelligent Software Agents*, chapter PET, 33–53 (The Hague: College Bescherming Persoonsgegevens).

Van Kleek M, OHara K (2014) The Future of Social is Personal: The Potential of the Personal Data Store. Miorandi D, Maltese V, Michael R, Nijholt A, Stewart J, eds., *Social Collective Intelligence*, 125–158 (Springer International Publishing).

Whitley EA (2009) Informational Privacy, Consent and the “Control” of Personal Data. *Information Security Technical Report* 14(3):154–159.

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

Zhang J, Adomavicius G, Gupta A, Ketter W (2020) Consumption and Performance: Understanding Longitudinal Dynamics of Recommender Systems via an Agent-Based Simulation Framework. *Information Systems Research* 31(1):76–101.

Zyskind G, Nathan O, Pentland AS (2015) Decentralizing Privacy: Using Blockchain to Protect Personal Data. *2015 IEEE Security and Privacy Workshops*, 180–184 (San Jose, CA).

Appendix A

Appendix for Essay 1

A.1 Top-down Review of End-user PETs

The Table A.1 provides a list of relevant papers and their classifications of end-user privacy enhancing technologies (PETs).

A.2 Bottom-up Review of End-user PETs

In addition to the above review of end-user PETs from academic research, we conduct another review of end-user PETs available to individuals in practice in case there are new commercial technologies not captured by the academic literature. The majority of end-user PETs exist in the form of applications and web-extensions. Therefore, we search the keyword "privacy" in leading software app stores, namely, the Apple app store, the Google play store, and the Google web store. Relevant information, such as the name of the app, the app description, the feedback rating from consumers, the number rating, etc., are collected. In addition, we also analyze the database of privacy enhancing technologies from the Center for Internet and Society [1] and the list of PETs from the Electronic Privacy Information Center.[2] The applications and extensions are subject to bottom-up inductive open-coding for classification by manually checking the descriptions.

After carefully checking the descriptions for each application or extension, we first eliminated those irrelevant apps that do not aim at protecting consumers' privacy. Those apps or extensions which focus on the protection of privacy from other people

[1] The Center for Internet and Society: https://cyberlaw.stanford.edu/wiki/index.php/Main_Page

[2] EPIC online guide to practical privacy tools: https://epic.org/privacy/tools.html

Articles	**Classifications**
Fritsch (2007)	(1) Privacy Protection: pseudonymiser, anonymiser products and services, encryption tools, filters and blockers, track and evidences erasers (2) Privacy Management: information tools, administrative tools
Clarke (2009)	(1) Pseudo-PETs: privacy seals, P3P (2) Counter-Technology: counter one specific privacy threat (3) Savage PETs: provide untraceable anonymity (4) Gentle PETs: pseudonymity tools balanced with accountability and identity management
Diaz and Gürses (2012)	(1) Privacy as "contro": privacy settings, purpose-based access control, auditing (2) Privacy as "condifentialit": anonymous authentication protocols, anonymous communication networks, private information retrieval (3) Privacy as "practic": Platform for privacy preference (P3P), privacy mirrors
Shen and Pearson (2011)	PETs for anonymisation, PETs to protect network invasion, PETs for identity management, PETs for data processing, policy-checking PETs
Heurix et al. (2015)	Dimensions of information privacy-enhancing technologies: scenario, aspect, aim, foundation, data, TTP, reversibility
Fischer-Hbner and Berthold (2017)	(1) Data Minimization Technologies: anonymous communication: DC network, mix nets, AN.ON, onion routing/Tor; Application Level: blind signatures, zero-knowledge proofs, anonymous credentials, private information retrieval (2) Transparency-enhancing Technologies: Ex ante versus ex post transparency-enhancing tools
Division (2017)	Inform consent, data minimization, data tracking, anonymity, control, negotiate terms and conditions, technical enforcement, remote audit of enforcement

Table A.1: Existing Classifications of PETs from Literature

rather than from enterprises, such as file encryption apps and screen filter apps, are also removed. We then also removed those which focus on security protection, such as hacker and phishing websites protector. The number of end-user PETs from each source under each review step are presented in Table A.2.

Sources	Google Play Store	Apple Store	Google Web Store	CIS	EPIC
No.Search Results	245	244	200	70	132
No.Relevant	90	97	85	55	83
No.Unique	88	92	84	53	78
Total Unique	354				

Table A.2: Bottom-up Review Process

Among the remaining apps and extensions, we identified 5 categories. The first category comprises various blockers which mainly block third-party advertisement (pop-ups, statics, and video ads), unwanted content, various trackers, etc. The second category falls into communication anonymizers which include VPN, firewall, private search engine, anonymous email and social network. They are achieved by mainly embedding in anonymous networks or proxies, adding noise or perturbation, using fake or virtual identities. The third category comprises data cleaners which aim to remove individuals' privacy-related data, such as browsing history, cookies, cache, adware, EXIF information from your disks, browsers, and photos. The four category includes permission managers which allow you to view and control permissions required by each app on your smartphone and report a privacy score. The final category comprises privacy policy checkers which help to summarize various privacy policies or provide a privacy score. In general, our review of end-user privacy enhancing technologies (PETs) in practice is consistent with the top down academic literature review. The specific proportion of each category is presented in Figure A.1.

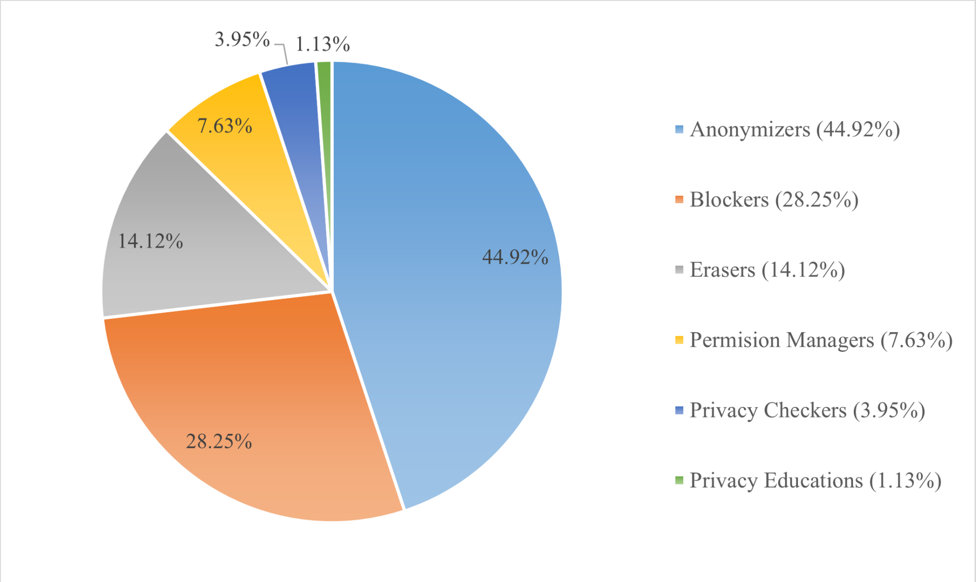


Figure A.1: Bottom-up Classification

A.3 Adoption Pattern Classification

In our simulation, we define three adoption patterns according to users' PETs adoption probability which is related to each user's rating frequency. Table A.3 presents the specific PETs adoption probability we assign to a user with rating frequency f_i under three adoption patterns. f_i is the number of user i's observations divided by total observations (here, 100,000). We are not intended to claim that this is the only way to calculate and assign adoption probability. There could be many ways to assign adoption probability that is consistent with the definition of our three adoption patterns.

	Adoption Probability
High-Sensitive	f_i
Uniform	$\frac{1}{100{,}000}$
Low-Sensitive	$\frac{1/f_i}{\sum_{i=1}^{100{,}000} 1/f_i}$

Table A.3: Adoption Probability under Different Adoption Patterns

Figure A.2 visualizes different adoption patterns under the above adoption probabilities assignment methodology. Users are ordered by their rating frequency f_i from lowest ("user 1") to highest ("user n") in the x-axis.

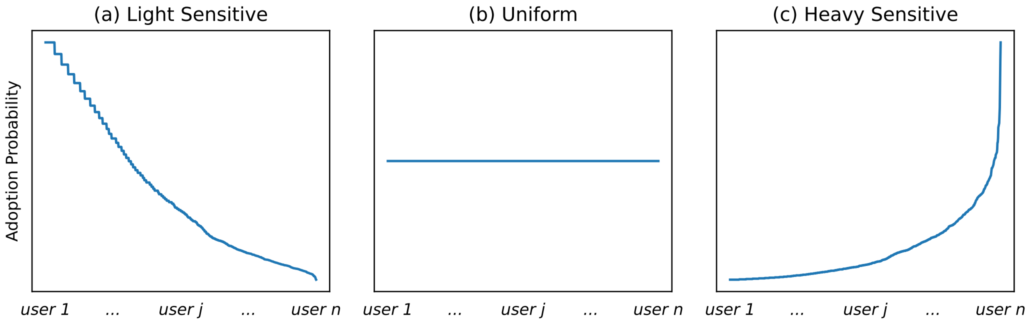


Figure A.2: Adoption Patterns

A.4 Robustness Check - MAE

In this section, we conduct a robustness check for our results using another evaluation metric – Mean Absolute Error (MAE) which is defined as follow:

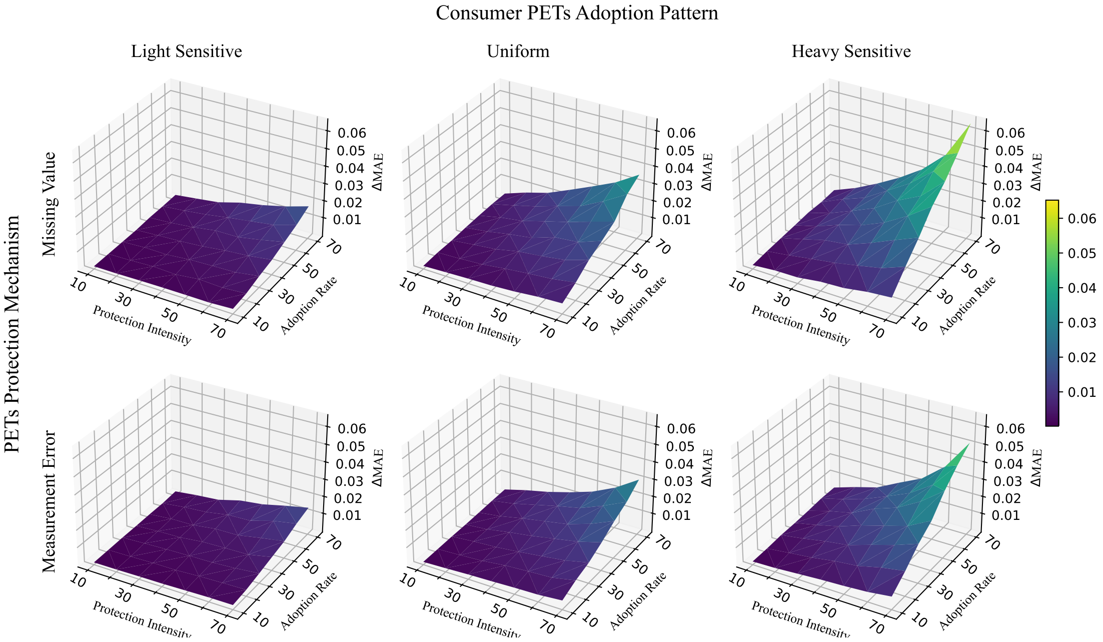
$$\sum_u \sum_i |r_{ui} - \hat{r}_{ui}|$$

where u stands for "users", i stands for "items". r_{ui} is actual user u's rating over item i, while $\hat{r}_{ui}$ is our predicted user u's rating over item i.

A.4.1 Main Results using MAE

Figure A.3 shows that our previous main results using RMSE are also consistent with results evaluated by another metric – MAE.

Figure A.3: Main Results using MAE



A.4.2 Regression Analysis using MAE

We also conduct regression analysis using mean absolute error (MAE) as dependent variable. In comparing Table A.4 to Table 2.2, it shows that all our results are still consistent.

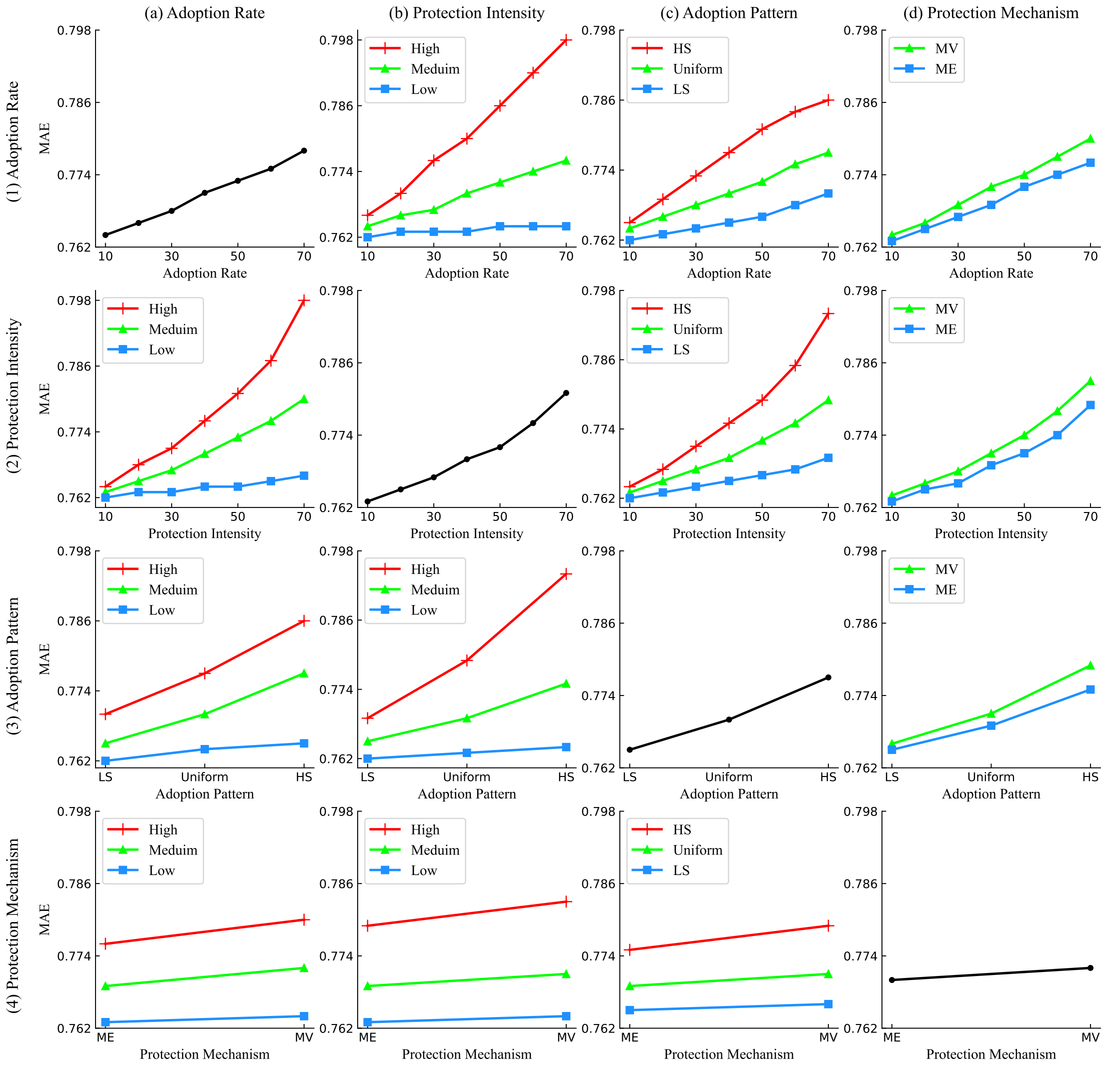
Table A.4: Regression Results using MAE

	ΔMAE		ΔMAE_{use}		ΔMAE_{del}	
$Variables$	(1)	(2)	(3)	(4)	(5)	(6)
$AdoptionRate$	0.024^{***}	0.020^{***}	-0.043^{***}	-0.003	0.062^{***}	0.010^{***}
	(0.000)	(0.000)	(0.003)	(0.006)	(0.001)	(0.003)
$ProtectionIntensity$	0.029^{***}	0.023^{***}	0.041^{***}	0.040^{***}	-0.034^{***}	-0.031^{***}
	(0.000)	(0.000)	(0.003)	(0.006)	(0.001)	(0.003)
$Adoption_{HS}$	0.006^{***}	0.006^{***}	-0.044^{***}	-0.045^{***}	0.044^{***}	0.042^{***}
	(0.000)	(0.000)	(0.001)	(0.002)	(0.001)	(0.001)
$Adoption_{LS}$	-0.005^{***}	-0.004^{***}	0.035^{***}	0.037^{***}	-0.008^{***}	-0.009^{***}
	(0.000)	(0.000)	(0.001)	(0.002)	(0.001)	(0.001)
$Protection_{MV}$	0.002^{***}	0.002^{***}	-0.001	0.000	0.002^{***}	0.001
	(0.000)	(0.000)	(0.001)	(0.002)	(0.001)	(0.001)
$AdoptionRate$		0.079^{***}		0.021		-0.097^{***}
$\times ProtectionIntensity$		(0.001)		(0.014)		(0.007)
$AdoptionRate$		0.013^{***}		-0.123^{***}		0.168^{***}
$\times Adoption_{HS}$		(0.000)		(0.007)		(0.003)
$AdoptionRate$		-0.011^{***}		-0.003		-0.029^{***}
$\times Adoption_{LS}$		(0.000)		(0.007)		(0.003)
$AdoptionRate$		0.005^{***}		0.005		0.011^{***}
$\times Protection_{MV}$		(0.000)		(0.006)		(0.003)
$ProtectionIntensity$		0.022^{***}		0.002		-0.031^{***}
$\times Adoption_{HS}$		(0.000)		(0.007)		(0.003)
$ProtectionIntensity$		-0.015^{***}		0.004		0.017^{***}
$\times Adoption_{LS}$		(0.000)		(0.007)		(0.003)
$ProtectionIntensity$		0.006^{***}		-0.002		0.003
$\times Protection_{MV}$		(0.000)		(0.006)		(0.003)
$Adoption_{HS}$		0.002^{***}		0.002		0.004^{***}
$\times Protection_{MV}$		(0.000)		(0.003)		(0.001)
$Adoption_{LS}$		-0.001		-0.005^{*}		-0.000
$\times Protection_{MV}$		(0.000)		(0.003)		(0.001)
$constant$	0.008^{***}	0.008^{***}	0.012^{***}	0.011^{***}	0.002^{***}	0.003^{***}
	(0.000)	(0.000)	(0.001)	(0.001)	(0.001)	(0.001)
R^2	0.593	0.777	0.108	0.120	0.221	0.322
Observations	29,400	29,400	29,390	29,390	29,400	29,400

Significance Levels: $^{***}\, p < 0.01$; $^{**}\, p < 0.05$; $^{*}\, p < 0.1$

The main effect of these four contingent factors and their interaction effect are visualized in A.4 when the recommendation performance is evaluated by mean absolute error (MAE). The results are consistent with 2.5.

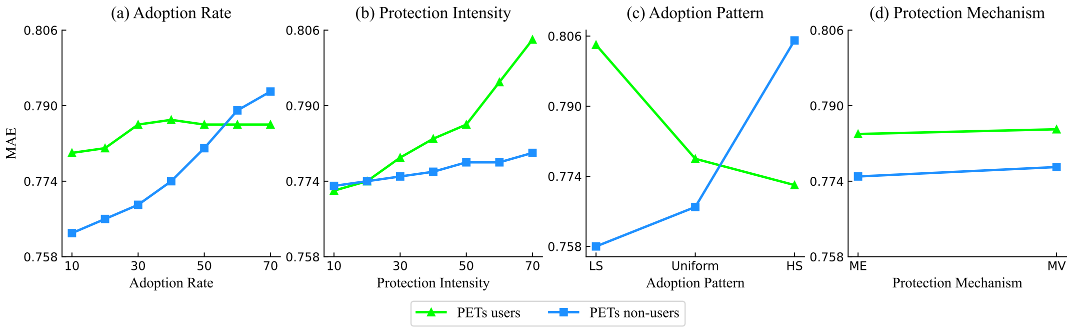
Figure A.4: Impact of End-user PET Adoption on *MAE*



A.4.3 Spillover Effect using MAE

When our recommendation accuracy is evaluated in MAE, the spillover effect is still significant (model (3) and (4) in Table A.4 where the dependent variable is the difference between average MAE for PETs users and average MAE for PETs non-users). The moderating effects of those four contingent factors on MAE in Figure A.5 are consistent with those in Figure 2.6.

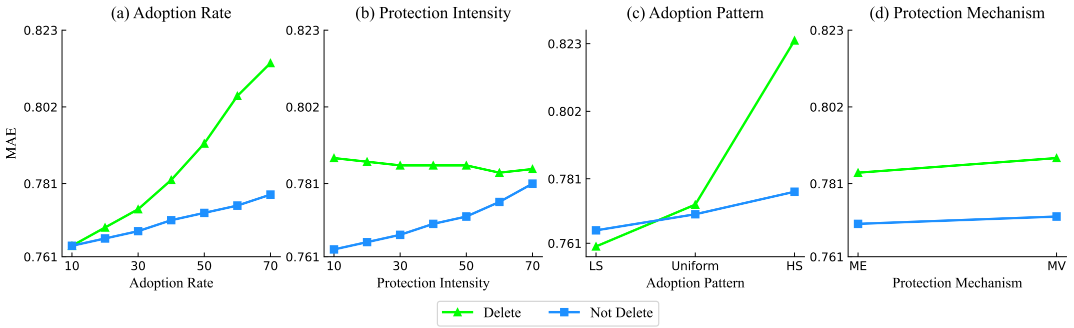
Figure A.5: Comparison between PET users and PET Non-users Under MAE



A.4.4 To Delete or Not to Delete using MAE

The effect of deleting all PETs users' observation from model training are also evaluated by MAE in this section. All results in RMSE are still consistent when we use another evaluation metric - MAE.

Figure A.6: Comparison between Deleting and Not Deleting PET Users' Observations in MAE



A.5 Robustness Check - NDCG

In this section, we conduct robustness check for our results using another evaluation metric – Normalized Discounted Cumulative Gain (NDCG) which is defined as follow:

$$nDCG(L,u) = \frac{DCG(L,u)}{DCG(L_{ideal},u)}$$

$$DCG(L,u) = \sum_{i}^{|L|} \frac{r_{ui}}{d(i)}$$

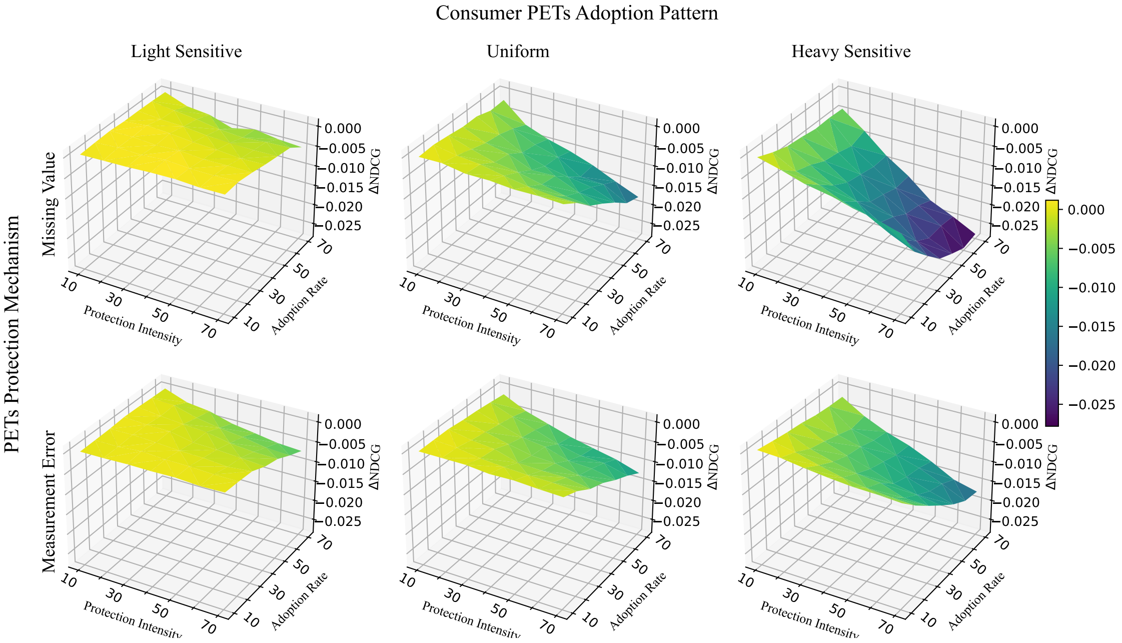
where "L" is the list of recommended items, $|L|$ is the number of recommended items, "u" stands for the user "u", r_{ui} is the real user u's rating on movie i, $d(i)$ is a discounted factor which is equal to $log_2(i+1)$ where i is the location of recommended item i.

Normalized Discounted Cumulative Gain ($NDCG$) is a measure of ranking quality. Different from $RMSE$ and MAE, higher $NDCG$ indicated higher recommendation performance.

A.5.1 Main Results using NDCG

Figure A.7 shows the impact of end-user PETs adoption on recommendation performance evaluated by $NDCG$. Our results using $RMSE$ (Figure 2.4) and MAE (Figure A.3) are still consistent when we evaluate the recommendation performance by NDCG (Figure A.7).

Figure A.7: Main Results using NDCG



A.5.2 Regression Analysis using NDCG

The regression results using $NDCG$ (Table A.5) as dependent variable are still consistent with the regression results using $RMSE$ (Table 2.2) and MAE (Table A.4)..

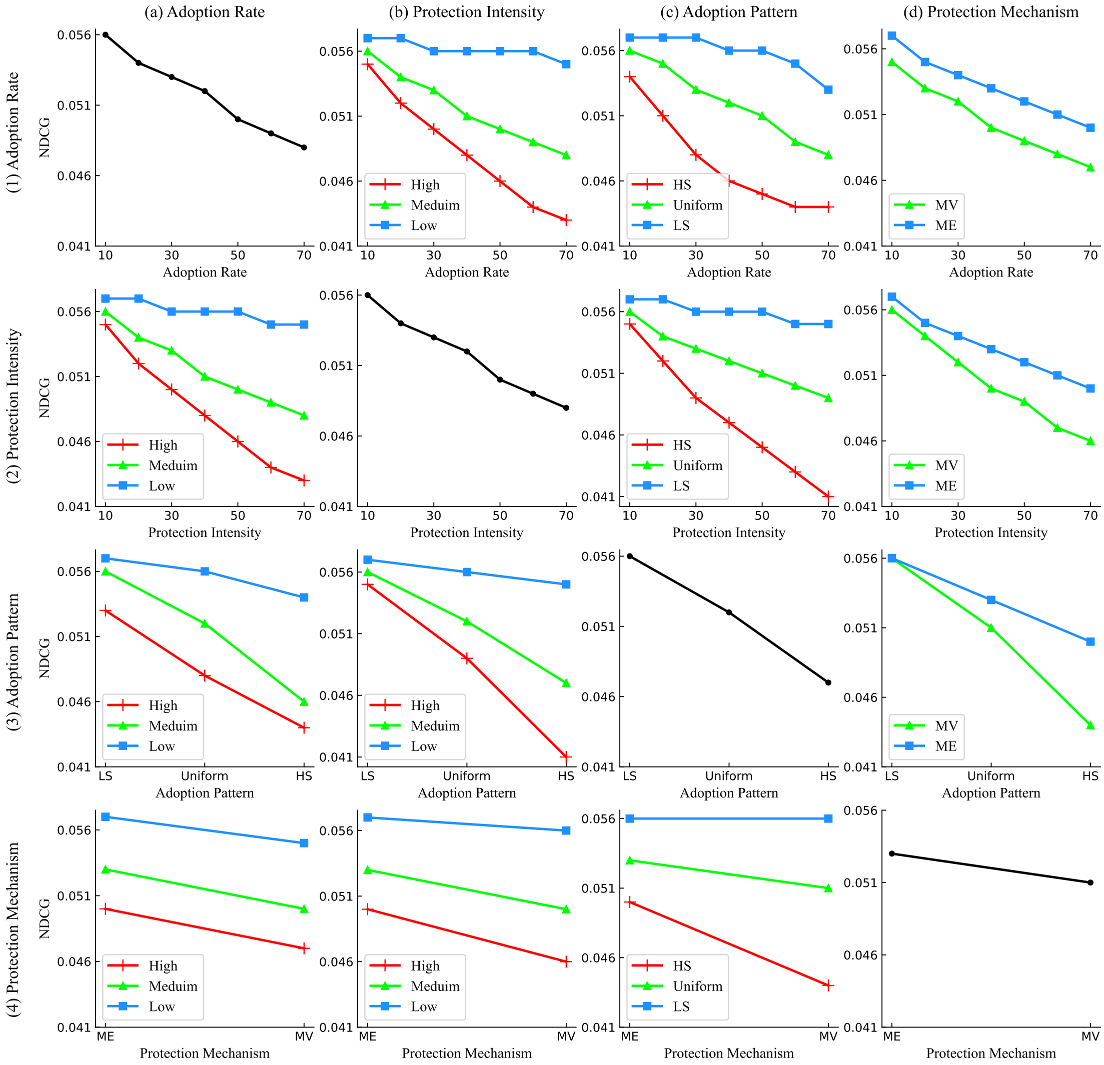
Table A.5: Regression Results using NDCG

	$\Delta NDCG$		$\Delta NDCG_{use}$		$\Delta NDCG_{del}$	
$Variables$	(1)	(2)	(3)	(4)	(5)	(6)
$AdoptionRate$	-0.013^{***}	-0.013^{***}	0.007^{***}	0.002^{**}	-0.001^{***}	0.002^{***}
	(0.000)	(0.000)	(0.000)	(0.001)	(0.000)	(0.000)
$ProtectionIntensity$	-0.013^{***}	-0.010^{***}	-0.018^{***}	-0.021^{***}	0.018^{***}	0.018^{***}
	(0.000)	(0.000)	(0.000)	(0.001)	(0.000)	(0.000)
$Adoption_{HS}$	-0.005^{***}	-0.003^{***}	0.006^{***}	0.006^{***}	-0.011^{***}	-0.009^{***}
	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)
$Adoption_{LS}$	0.004^{***}	0.003^{***}	-0.005^{***}	-0.005^{***}	0.005^{***}	0.004^{***}
	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)
$Protection_{MV}$	-0.003^{***}	-0.002^{***}	0.001^{***}	0.001^{***}	-0.001^{***}	-0.001^{***}
	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)
$AdoptionRate$		-0.028^{***}		0.010^{***}		0.033^{***}
$\times ProtectionIntensity$		(0.001)		(0.002)		(0.001)
$AdoptionRate$		-0.003^{***}		0.015^{***}		-0.018^{***}
$\times Adoption_{HS}$		(0.000)		(0.001)		(0.001)
$AdoptionRate$		0.008^{***}		0.000		0.011^{***}
$\times Adoption_{LS}$		(0.000)		(0.001)		(0.001)
$AdoptionRate$		-0.003^{***}		0.001		-0.002^{***}
$\times Protection_{MV}$		(0.000)		(0.001)		(0.000)
$ProtectionIntensity$		-0.011^{***}		0.000		0.018^{***}
$\times Adoption_{HS}$		(0.000)		(0.001)		(0.001)
$ProtectionIntensity$		0.009^{***}		0.004^{***}		-0.014^{***}
$\times Adoption_{LS}$		(0.000)		(0.001)		(0.001)
$ProtectionIntensity$		-0.006^{***}		0.004^{***}		-0.003^{***}
$\times Protection_{MV}$		(0.000)		(0.001)		(0.000)
$Adoption_{HS}$		-0.004^{***}		0.000		-0.003^{***}
$\times Protection_{MV}$		(0.000)		(0.000)		(0.000)
$Adoption_{LS}$		0.003		-0.000		0.002^{***}
$\times Protection_{MV}$		(0.000)		(0.000)		(0.000)
$constant$	-0.004^{***}	-0.004^{***}	-0.009^{***}	-0.009^{***}	0.000^{***}	0.000^{*}
	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)
R^2	0.586	0.736	0.129	0.138	0.385	0.496
Observations	29,400	29,400	29,390	29,390	29,400	29,400

Significance Levels: $^{***}p < 0.01$; $^{**}p < 0.05$; $^{*}p < 0.1$

The interaction effect of these four contingent factors are visualized in Figure A.8. The results are consistent with those using RMSE (Figure 2.5) and MAE (Figure A.4).

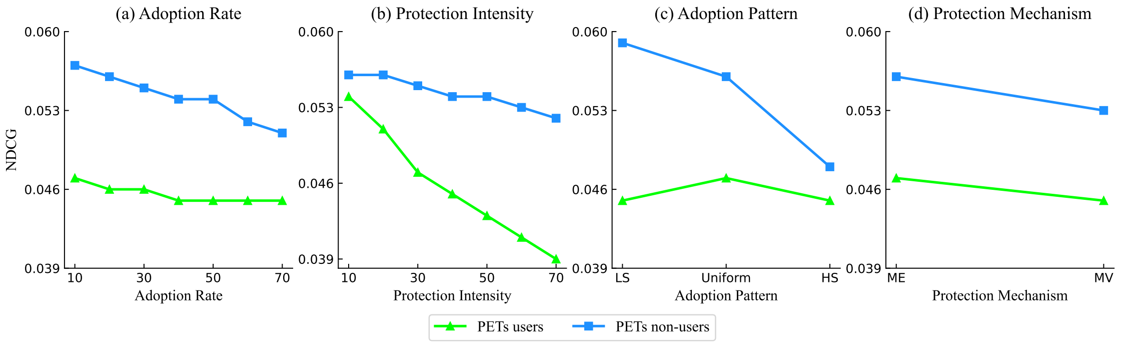
Figure A.8: Impact of End-user PET Adoption on *NDCG*



A.5.3 Spillover Effect using NDCG

The spillover effect still exists and is consistent when the recommendation performance is evaluated by *NDCG* (Figure A.9).

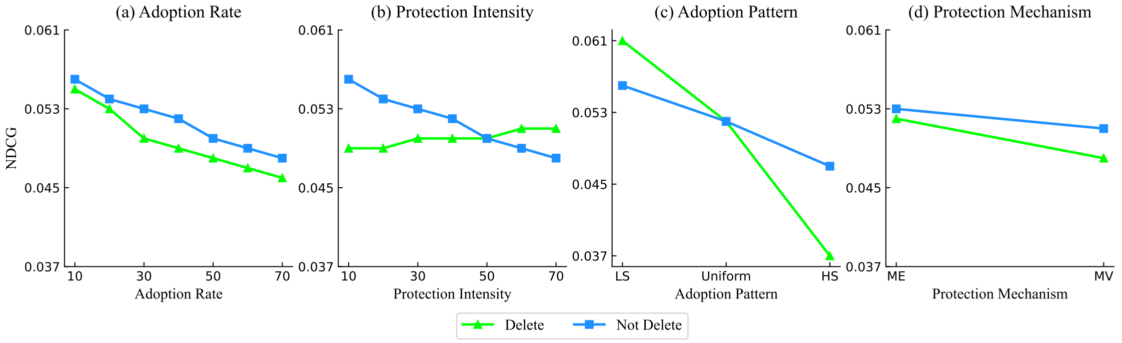
Figure A.9: Comparison between PET users and PET Non-users Under NDCG



A.5.4 To Delete or Not to Delete using NDCG

The regression results (Table A.5, model (5) and (6)) seem to fail to support our conclusion that deleting all PETs users observation from model training is not a good idea when the recommendation performance is evaluated by another metric - NDCG (the constant term is near to 0). The NDCG with and without PETs users' observation are quite similar (Figure A.6(a) and (d)). The interesting finding is that, when the protection intensity is low, keeping PETs users' observation is better; however, when the protection intensity is high, deleting all PETs users' observation will get a higher model performance (higher $NDCG$).

Figure A.10: Comparison between Deleting and Not Deleting PET Users' Observations in NDCG



A.6 Statistics Summary for Regression Variables

Table A.6 provides the statistics summary of key variables we use in our regression analysis.

A.7 Robustness Check - User-based Collaborative Filtering

We also conduct robustness check in another recommendation algorithm – user-base collaborative filtering. In this section, to simplify the presentation, we only present the simulation results using – RMSE. The results are consistent when the recommendation performance is evaluated by MAE and NDCG.

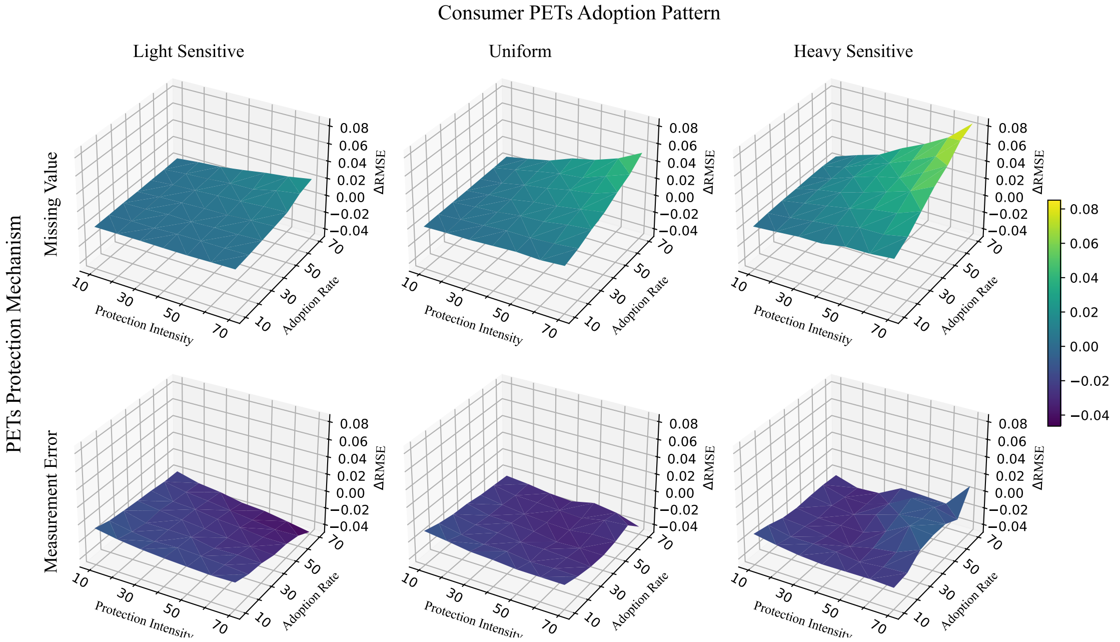
A.7.1 Main Results

As shown in Figure A.11, the impact of adoption rate, protection intensity and adoption pattern on recommendation performance using user-based collaborative filtering algorithm is consistent with their impact using item-based collaborative filtering algorithm. Nevertheless, the impact of protection mechanism is different. Under user-based collaborative filtering algorithm, the measurement error protection mechanism seems to improve recommendation performance.

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)	Mean	Std
(1) $\Delta RMSE$	1														0.01	0.01
(2) $\Delta RMSE_{use}$	-0.17	1													0.01	0.15
(3) $\Delta RMSE_{del}$	0.23	-0.74	1												0.03	0.09
(4) ΔMAE	0.99	-0.18	0.24	1											0.01	0.01
(5) ΔMAE_{use}	-0.10	0.94	-0.65	-0.10	1										0.01	0.10
(6) ΔMAE_{del}	0.17	-0.71	0.95	0.17	-0.71	1									0.02	0.06
(7) $\Delta NDCG$	-0.74	0.26	-0.31	-0.73	0.18	-0.25	1								-0.01	0.01
(8) $\Delta NDCG_{use}$	0.07	-0.21	0.24	0.07	-0.14	0.20	-0.13	1							-0.01	0.02
(9) $\Delta NDCG_{del}$	-0.04	0.33	-0.43	-0.03	0.24	-0.37	0.11	-0.50	1						-0.00	0.01
(10) $ProtectionIntensity$	0.42	-0.07	0.21	0.41	-0.08	0.21	-0.37	0.09	-0.02	1					0.4	0.2
(11) $AdoptionRate$	0.51	0.07	-0.10	0.50	0.08	-0.12	-0.38	-0.21	0.30	0.00	1				0.4	0.2
(12) $Adoption_{HS}$	0.37	-0.42	0.50	0.36	0.28	0.40	-0.46	0.24	-0.52	0.00	-0.00	1			0.33	0.47
(13) $Adoption_{LS}$	-0.34	0.38	-0.32	-0.33	0.26	-0.25	0.44	-0.23	0.40	0.00	0.00	-0.50	1		0.33	0.47
(14) $Protection_{MV}$	0.10	-0.01	0.02	0.10	-0.00	0.02	-0.18	0.03	-0.04	-0.00	-0.00	-0.00	-0.00	1	0.5	0.5

Table A.6: Statistics Summary

Figure A.11: Main Results using RMSE in User-based Collaborative Filtering



A.7.2 Regression Analysis

In this section, we conduct robustness checks for our regression analysis using data from user-based collaborative filtering algorithm. Table A.7 provides statistics summary of key variables for regression analysis in this section.

The regression results using user-based collaborative filtering algorithm (Table A.8) are consistent with those using item-based collaborative filtering algorithm (Table 2.2).

The majority of interaction effect among those four contingent factors are still consistent in Figure A.12 comparing to Figure 2.5 except for the interaction between adoption rate (protection intensity) and protection mechanism (measurement error).

A.7.3 Spillover Effect

The spillover effect still exists when we use user-based collaborative filtering algorithm (figure A.13, Model (3) and (4) in Table A.8).

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)	Mean	Std
(1) $\Delta RMSE$	1														-0.00	0.02
(2) $\Delta RMSE_{use}$	-0.01	1													0.01	0.13
(3) $\Delta RMSE_{del}$	0.14	-0.45	1												0.00	0.10
(4) ΔMAE	0.97	-0.02	0.12	1											0.00	0.02
(5) ΔMAE_{use}	0.02	0.95	-0.43	0.02	1										0.01	0.12
(6) ΔMAE_{del}	0.09	-0.50	0.95	0.07	-0.53	1									-0.00	0.08
(7) $\Delta NDCG$	-0.66	0.03	-0.22	-0.55	0.06	-0.21	1								0.00	0.01
(8) $\Delta NDCG_{use}$	0.14	0.04	0.05	0.09	0.06	0.03	-0.28	1							-0.01	0.01
(9) $\Delta NDCG_{del}$	-0.09	0.05	0.07	-0.06	0.03	0.01	0.22	-0.40	1						-0.00	0.01
(10) $ProtectionIntensity$	0.08	-0.01	-0.02	0.16	-0.02	-0.01	0.08	-0.00	-0.11	1					0.4	0.2
(11) $AdoptionRate$	0.14	0.05	-0.10	0.23	0.06	-0.12	0.12	-0.29	0.31	-0.00	1				0.4	0.2
(12) $Adoption_{HS}$	0.19	-0.04	0.07	0.26	0.09	-0.00	0.08	0.04	-0.09	-0.00	-0.00	1			0.33	0.47
(13) $Adoption_{LS}$	-0.14	0.04	-0.05	-0.20	-0.06	0.01	-0.07	-0.05	0.09	0.00	0.00	-0.50	1		0.33	0.47
(14) $Protection_{MV}$	0.76	0.01	0.15	0.66	-0.00	0.13	-0.69	0.15	-0.13	0.00	0.00	0.00	-0.00	1	0.5	0.5

Table A.7: Statistics Summary - User-based Collaborative Filtering

Table A.8: Regression Results using RMSE in User-based Collaborative Filtering

	$\Delta RMSE$		$\Delta RMSE_{use}$		$\Delta RMSE_{del}$	
$Variables$	(1)	(2)	(3)	(4)	(5)	(6)
$AdoptionRate$	0.010^{***} (0.001)	-0.017^{***} (0.001)	-0.007 (0.005)	0.024^{**} (0.011)	-0.011^{**} (0.004)	-0.102^{***} (0.008)
$ProtectionIntensity$	0.018^{***} (0.001)	-0.013^{***} (0.001)	0.032^{***} (0.005)	0.009 (0.011)	-0.051^{***} (0.004)	-0.049^{***} (0.008)
$Adoption_{HS}$	0.008^{***} (0.000)	0.005^{***} (0.000)	-0.006^{**} (0.003)	0.016^{***} (0.004)	0.015^{***} (0.002)	-0.014^{***} (0.003)
$Adoption_{LS}$	-0.003^{***} (0.000)	0.002^{***} (0.000)	0.009^{***} (0.003)	-0.007^{**} (0.004)	-0.003 (0.002)	0.005^{*} (0.003)
$Protection_{MV}$	0.037^{***} (0.000)	0.038^{***} (0.000)	0.003 (0.002)	0.006 (0.004)	0.030^{***} (0.002)	0.016^{***} (0.003)
$AdoptionRate$ $\times ProtectionIntensity$		0.071^{***} (0.002)		-0.014 (0.027)		-0.184^{***} (0.020)
$AdoptionRate$ $\times Adoption_{HS}$		0.021^{***} (0.001)		-0.118^{***} (0.013)		0.019^{*} (0.010)
$AdoptionRate$ $\times Adoption_{LS}$		-0.015^{***} (0.001)		0.027^{**} (0.013)		-0.012 (0.010)
$AdoptionRate$ $\times Protection_{MV}$		0.050^{***} (0.001)		-0.002 (0.011)		0.177^{***} (0.008)
$ProtectionIntensity$ $\times Adoption_{HS}$		0.036^{***} (0.001)		0.033^{**} (0.013)		-0.070^{***} (0.010)
$ProtectionIntensity$ $\times Adoption_{LS}$		-0.018^{***} (0.001)		0.014 (0.013)		0.026^{***} (0.010)
$ProtectionIntensity$ $\times Protection_{MV}$		0.050^{***} (0.001)		0.006 (0.011)		0.025^{***} (0.008)
$Adoption_{HS}$ $\times Protection_{MV}$		0.006^{***} (0.000)		-0.042^{***} (0.005)		0.057^{***} (0.004)
$Adoption_{LS}$ $\times Protection_{MV}$		-0.009^{***} (0.000)		0.032^{***} (0.005)		-0.017^{***} (0.004)
$constant$	-0.025^{***} (0.000)	-0.025^{***} (0.000)	0.004 (0.002)	0.024 (0.003)	-0.018^{***} (0.002)	-0.011^{***} (0.002)
R^2	0.650	0.814	0.005	0.027	0.037	0.103
Observations	14,675	14,675	14,675	14,675	14,675	14,675

Significance Levels: $^{***}\, p < 0.01$; $^{**}\, p < 0.05$; $^{*}\, p < 0.1$

Figure A.13: Comparison between PET users and PET Non-users Under $RMSE$ in User-based CF

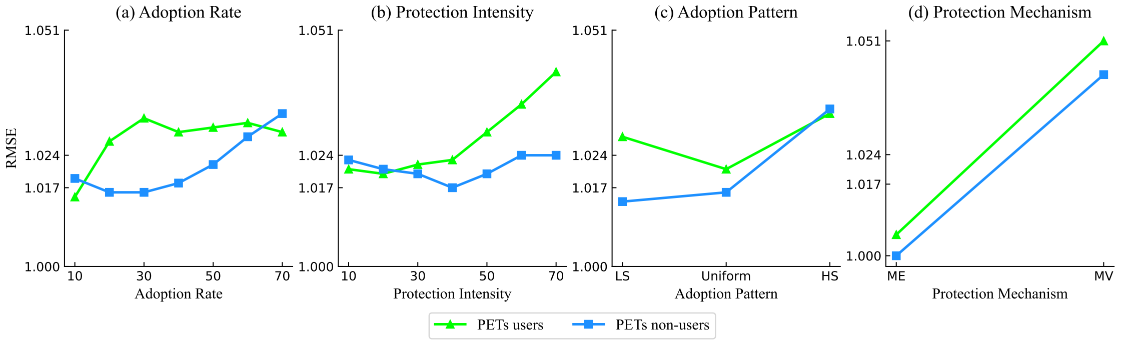
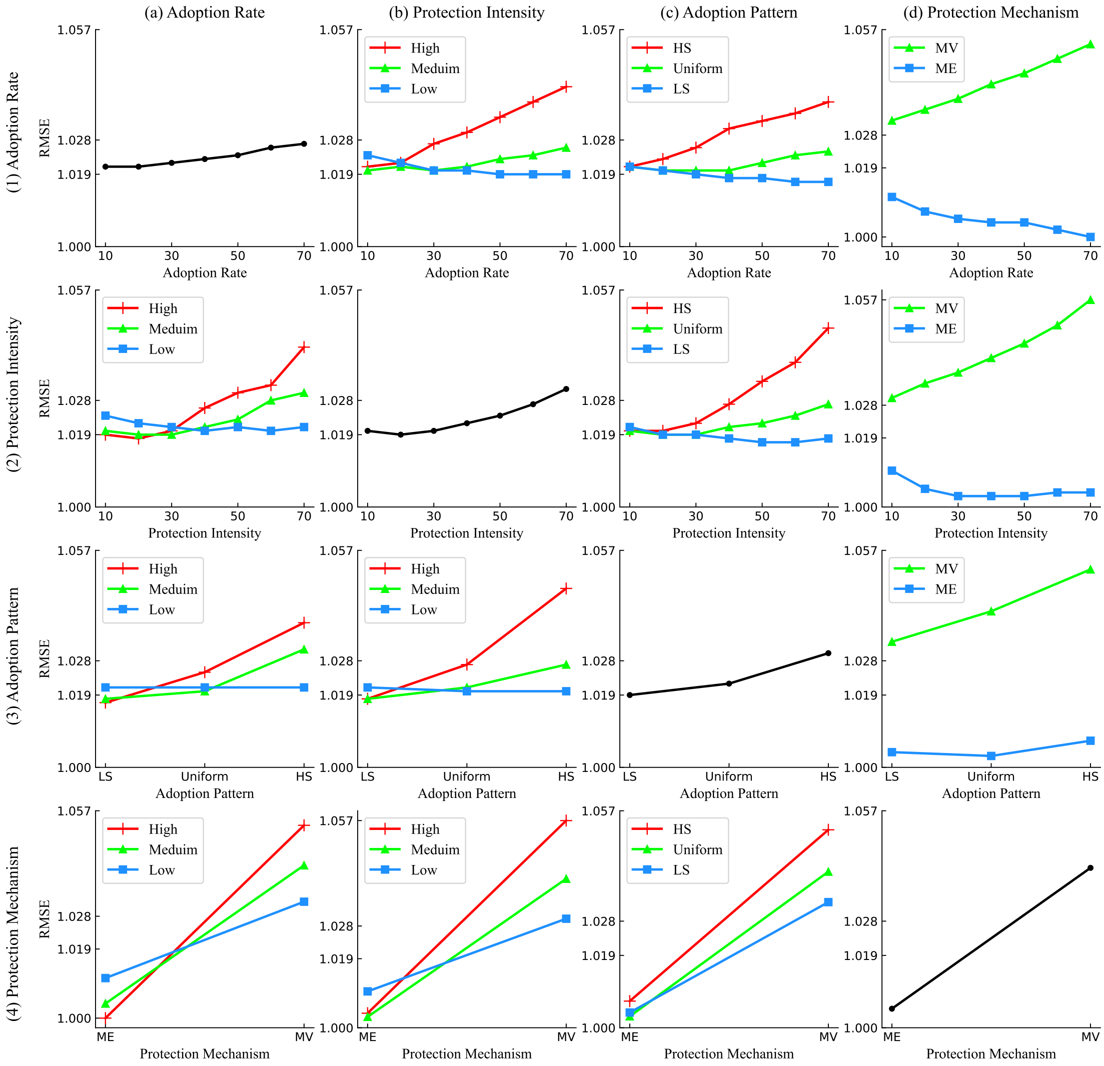


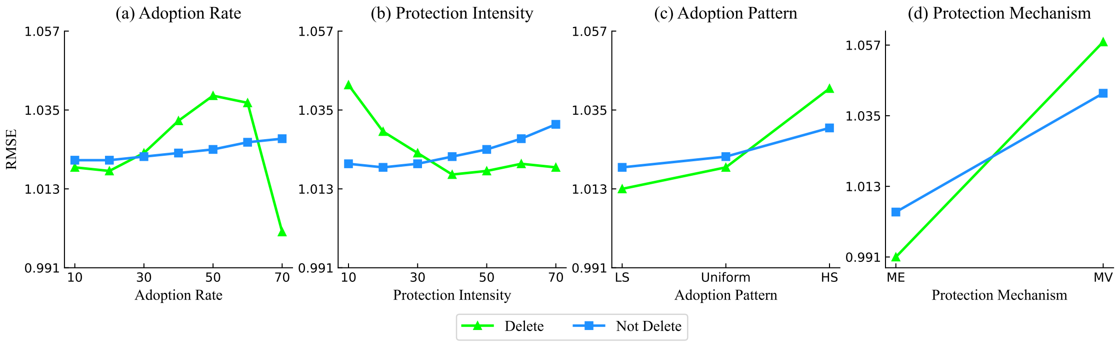
Figure A.12: Impact of End-user PET Adoption on *RMSE* in User-based Collaborative Filtering



A.7.4 To Delete or Not to Delete

The impact of deleting all PETs users' observation on recommendation performance is quite different using user-based collaborative filtering algorithm (Figure A.14) when comparing to the one using item-based collaborative filtering algorithm (Figure 2.7). It seems that whether to delete or not heavily depends on the recommendation algorithm.

Figure A.14: Comparison between Deleting and Not Deleting PET Users' Observations in $RMSE$ under User-based Collaborative Filtering



Appendix B

Appendix for Essay 2

This appendix provides the detailed mathematical derivation and proofs for the lemmas and propositions in Essay 2.

B.1 Proof of Lemma 1

B.1.1 Benchmark Equilibrium Solution

According to users' utilities in Table 3.1 and 3.2, the seller faces the following demand function:

$$D_{in} = D_{in}^{NS} + D_{in}^{S} = \begin{cases} (1-\alpha)(P_{out}+c), & 0 \le P_{out}+c \le 1 \\ 1-\alpha, & 1 < P_{out}+c \end{cases}$$

$$D_{out} = D_{out}^{NS} + D_{out}^{S} = \begin{cases} 1-(P_{out}+c), & 0 \le P_{out}+c \le 1 \\ 0, & 1 < P_{out}+c \end{cases}$$

The seller maximize the following profit with respect to P_{out}, where $P_{in}^{b*}(v) = v$:

$$\max_{P_{out}} \pi(P_{out}) = P_{out}D_{out} + \int P_{in}^{b*}(v) D_{in} dF(v)$$

(1) **Case 1:** $0 \le P_{out}+c \le 1$

We have the following maximization problem:

$$\begin{aligned} \max_{P_{out}} \pi(P_{out}) &= P_{out}(1-P_{out}-c) + (1-\alpha)\int_0^{P_{out}+c} v dv \\ &= P_{out}(1-P_{out}-c) + \frac{1}{2}(1-\alpha)(P_{out}+c)^2 \\ &= -\frac{1}{2}(1+\alpha)P_{out}^2 + (1-\alpha c)P_{out} + \frac{1}{2}(1-\alpha)c^2 \end{aligned}$$

The first order condition (FOC) is:

$$-(1+\alpha)P_{out} + (1-\alpha c) = 0$$

Since we have $0 \leq P_{out} + c \leq 1$, the optimal P_{out} is:

$$\widetilde{P}_{out} = min\left\{1-c, \frac{1-\alpha c}{1+\alpha}\right\} = \begin{cases} \dfrac{1-\alpha c}{1+\alpha}, & 0 \leq c < \alpha \leq 1 \\ 1-c, & 0 \leq \alpha \leq c \leq 1 \end{cases}$$

Thus, the equilibrium profit is:

$$\widetilde{\pi} = \begin{cases} \dfrac{1+c^2-2\alpha c}{2(1+\alpha)}, & 0 \leq c < \alpha \leq 1 \\ \dfrac{1-\alpha}{2}, & 0 \leq \alpha \leq c \leq 1 \end{cases}$$

(2) **Case 2:** $1 < P_{out} + c$

All privacy sensitive (S) users choose to opt-out and not buy the product. The profit only comes from privacy non-sensitive users who all choose to opt-in and buy the product.

$$\widetilde{\pi} = \frac{1-\alpha}{2}$$

For any $0 \leq \alpha \leq 1$ and $0 \leq c \leq 1$, we have

$$\frac{1+c^2-2\alpha c}{2(1+\alpha)} - \frac{1-\alpha}{2} = \frac{(c-\alpha)^2}{2(1+\alpha)} \geq 0$$
$$\frac{1+c^2-2\alpha c}{2(1+\alpha)} \geq \frac{1-\alpha}{2}$$

Taken together, the benchmark equilibrium solution without PDP is:

(1) Low privacy concern $(0 \leq \alpha \leq c \leq 1)$

- $P_{in}^{b*}(v) = v$, $P_{out}^{b*} \geq 1-c$
- $\pi^{b*} = \dfrac{1-\alpha}{2}$, $CS^{b*} = 0$, $TW^{b*} = \dfrac{1-\alpha}{2}$

(2) High privacy concern $(0 \leq c < \alpha \leq 1)$

- $P_{in}^{b*}(v) = v$, $P_{out}^{b*} = \dfrac{1-\alpha c}{1+\alpha}$
- $\pi^{b*} = \dfrac{1+c^2-2\alpha c}{2(1+\alpha)}$, $CS^{b*} = \dfrac{(\alpha-c)^2}{2(1+\alpha)^2}$, $TW^{b*} = \dfrac{(\alpha-c)^2+(1+c^2-2\alpha c)(1+\alpha)}{2(1+\alpha)^2}$

B.1.2 Static Comparative Analysis in Benchmark Equilibrium

Under high privacy concern ($0 \leq c < \alpha \leq 1$), we have:

$$\text{User opt-in rate: } (P_{out}^{b*} + c)(1-\alpha) = \frac{(1+c)(1-\alpha)}{1+\alpha}$$

$$\begin{aligned}
\frac{\partial P_{out}^{b*}}{\partial \alpha} &= -\frac{1+c}{(1+\alpha)^2} < 0, & \frac{\partial P_{out}^{b*}}{\partial c} &= -\frac{\alpha}{1+\alpha} \leq 0 \\
\frac{\partial \pi^{b*}}{\partial \alpha} &= -\frac{(1+c)^2}{2(1+\alpha)^2} < 0, & \frac{\partial \pi^{b*}}{\partial c} &= \frac{c-\alpha}{1+\alpha} \leq 0 \\
\frac{\partial CS^{b*}}{\partial \alpha} &= \frac{(\alpha-c)(1+c)}{(1+\alpha)^3} \geq 0, & \frac{\partial CS^{b*}}{\partial c} &= \frac{c-\alpha}{(1+\alpha)^2} \leq 0 \\
\frac{\partial TW^{b*}}{\partial \alpha} &= \frac{(1+c)[(\alpha-1)-(3+\alpha)c]}{2(1+\alpha)^3} \leq 0, & \frac{\partial TW^{b*}}{\partial c} &= \frac{(c-\alpha)(2+\alpha)}{(1+\alpha)^2} \leq 0
\end{aligned}$$

Thus, the proportion of opt-in users is decreasing in α but increasing in c. P_{out}^{b*}, π^{b*} and TW^{b*} are decreasing in α and c. CS^{b*} is increasing in α but decreasing in c.

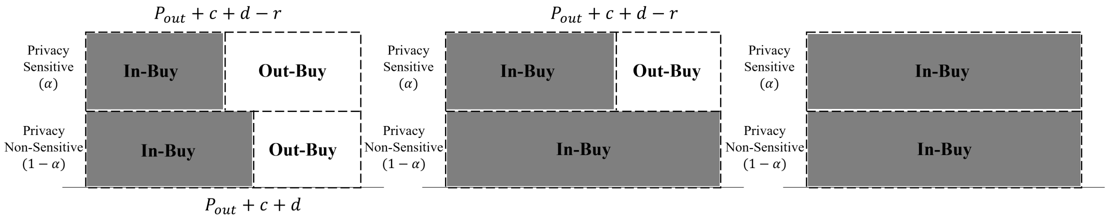
B.2 Proof of Lemma 2

In this section, we drive the equilibrium solution when users are naïve. In order to find the optimal P_{out}^{n*} and d^{n*}, we firstly need to figure out the users demand given any P_{out} and d. The users demand depends on the magnitude of d and P_{out}.

Case 1: $d \geq r$

According to users' utilities in Table 3.1 and 3.2, both privacy sensitive and privacy non-sensitive users choose to either "Opt-in and Buy" or "Opt-out and Buy". The market segmentation is presented in the following figure.

Figure B.1: Naïve Users Segmentation ($d \geq r$)


$P_{out}+c+d-r$
Privacy Sensitive (α)
In-Buy
Out-Buy
Privacy Non-Sensitive ($1-\alpha$)
In-Buy
Out-Buy
$P_{out}+c+d$
$P_{out}+c+d-r$
Privacy Sensitive (α)
In-Buy
Out-Buy
Privacy Non-Sensitive ($1-\alpha$)
In-Buy
Privacy Sensitive (α)
In-Buy
Privacy Non-Sensitive ($1-\alpha$)
In-Buy

(1) $0 \leq P_{out} \leq 1-c-d$ **(2) $1-c-d < P_{out} \leq 1-c-d+r$** **(3) $1-c-d+r < P_{out}$**

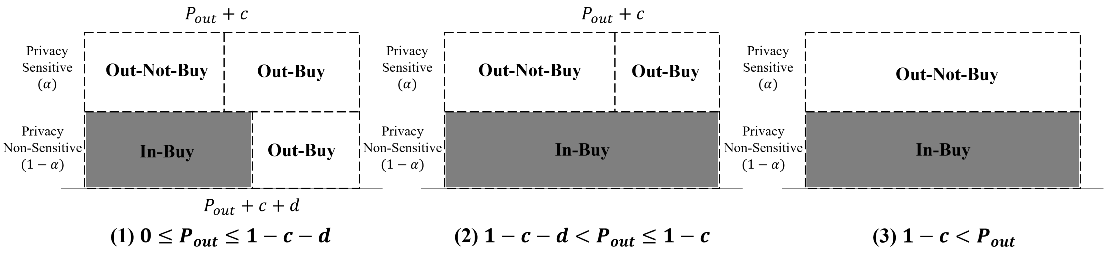
Because (1) the seller can extract more surplus from making a single user to choose "Opt-in and Buy" rather than "Opt-out and Buy", and (2) there is no credibility loss or market shrinkage, the seller will maximize his profit by setting a extremely high P_{out}^{n*} such that all users choose “Opt-out and Buy”. Therefore, in this case, the sub-optimal solution is:

$$\begin{aligned} \widetilde{d}^{n} &\geq r \\ \widetilde{P}_{out}^{n} &> 1 - c - d + r \\ \widetilde{\pi}^{n} &= \int_{0}^{1} v dv = \frac{1}{2} \end{aligned}$$

Case 2: $0 \leq d < r$

This case is similar to the benchmark setting where there are some privacy sensitive (S) users choose to opt-out and not buy the product. There are three sub-cases.

Figure B.2: Naïve Users Segmentation ($0 \leq d < r$)


$P_{out} + c$
Privacy Sensitive (α)
Out-Not-Buy
Out-Buy
Privacy Non-Sensitive ($1-\alpha$)
In-Buy
Out-Buy
$P_{out} + c + d$
$P_{out} + c$
Privacy Sensitive (α)
Out-Not-Buy
Out-Buy
Privacy Non-Sensitive ($1-\alpha$)
In-Buy
Privacy Sensitive (α)
Out-Not-Buy
Privacy Non-Sensitive ($1-\alpha$)
In-Buy

(1) $0 \leq P_{out} \leq 1 - c - d$ **(2) $1 - c - d < P_{out} \leq 1 - c$** **(3) $1 - c < P_{out}$**

Obviously, the market cannot be fully covered for any value of P_{out} when $0 \leq d < r$. There are always some privacy sensitive users with low valuation choose to “Opt-out and Not-buy”. Thus, the seller’s profit is always smaller than $\frac{1}{2}$.

Taken together, when all users are naïve, the equilibrium solution is:

$$\begin{aligned} P_{in}^{n*}(v) &= v \\ P^{n*} &\geq 1 - c - d^{n*} - r \\ d^{n*} &\geq r \\ \pi^{n*} &= \frac{1}{2} \\ CS^{n*} &= \alpha r \\ TW^{n*} &= \frac{1 - 2\alpha r}{2} \end{aligned}$$

B.3 Proof of Lemma 3

Case 1: $d \geq r$

In this case, according to users' utility (Table 3.1 and 3.2), both privacy sensitive and privacy non-sensitive users will choose to either "Opt-in and Buy" or "Opt-out and Buy". Given any specific d (where $d \geq r$), according to Figure B.1, the seller will set a high P_{out} (specifically, $P_{out} \geq 1-c-d+r$) such that both privacy sensitive and privacy non-sensitive users will choose to "Opt-in and Buy". Therefore, the seller's profit is:

$$\pi(d) = (1-d)\int_0^1 v dv = \frac{1-d}{2}$$

It is decreasing in the PDP level d. Since $d \geq r$, in this case, the sub-optimal solution is:

$$\begin{aligned} \widetilde{P}^s_{in}(v) &= v \\ \widetilde{P}^s_{out} &\geq 1-c \\ \widetilde{d}^s &= r \\ \widetilde{\pi}^s &= \frac{1-r}{2} \end{aligned}$$

Case 2: $0 \leq d < r$

According to Figure B.2, there are three cases for the users demand.

(1) $0 \leq P_{out} \leq 1-c-d$

The seller faces the following profit function:

$$\begin{aligned} \pi(P_{out}, d) = \{&\underbrace{\alpha P_{out}(1-P_{out}-c)}_{\text{Profit from } S \text{ users}} \\ &\underbrace{+ (1-\alpha)\left[\int_0^{P_{out}+c+d} vdv + P_{out}(1-P_{out}-c-d)\right]}_{\text{Profit from } NS \text{ users}}\}(1-d) \end{aligned}$$

Using backward induction, given d, the seller firstly maximizes his profit with respect to P_{out}.

$$\frac{\partial \pi}{\partial P_{out}} = \left[(1-\alpha c) - (1+\alpha)P_{out}\right](1-d)$$

Since $0 \leq P_{out} \leq 1-c-d$, we have:

$$\widetilde{P}_{out} = \min\left\{1-c-d, \quad \frac{1-\alpha c}{1+\alpha}\right\}$$

Since

$$(1-c-d)-\frac{1-\alpha c}{1+\alpha}=\frac{\alpha-c}{1+\alpha}-d$$

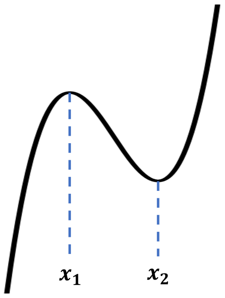
(a) When $0\le\alpha\le c\le 1$, $1-c-d\le(1-\alpha c)/(1+\alpha)$, we have:

$$\begin{aligned}
\widetilde{P}_{out} &= 1-c-d\\
\pi_1(d) &= \left[\alpha(1-c-d)d+(1-\alpha)\int_0^1 vdv\right](1-d)\\
&= \alpha d^3-\alpha(2-c)d^2+\frac{3\alpha-2\alpha c-1}{2}d+\frac{1-\alpha}{2}\\
\frac{\partial\pi_1(d)}{\partial d} &= 3\alpha d^2-2\alpha(2-c)d+\frac{3\alpha-2\alpha c-1}{2}\\
\Delta_1 &= [2\alpha(2-c)]^2-6\alpha(3\alpha-2\alpha c-1)=2\alpha\left[3-\alpha(1+2c-2c^2)\right]>0\\
& \quad for\ any\ (\alpha,\ c)\ in\ (0,\ 1)\times(0,\ 1)
\end{aligned}$$

$\pi_1(d)$ is a cubic function of d which has two extremum points $(x_1,\ x_2)$. Figure B.3 provides an illustration of such cubic function.

$$x_1=\frac{2\alpha(2-c)-\sqrt{\Delta_1}}{6\alpha}$$
$$x_2=\frac{2\alpha(2-c)+\sqrt{\Delta_1}}{6\alpha}$$

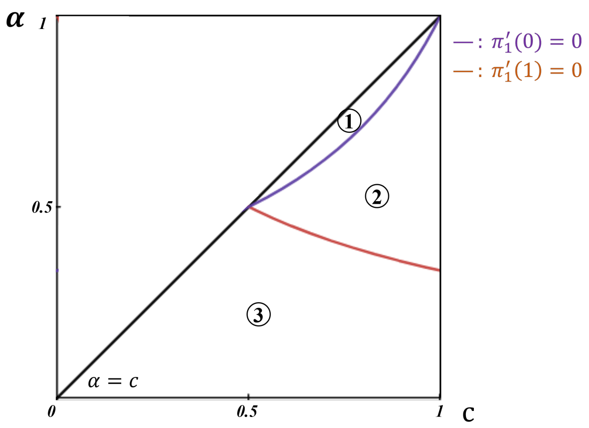
Figure B.3: Illustration of Cubic Profit Function 1



Notice that:

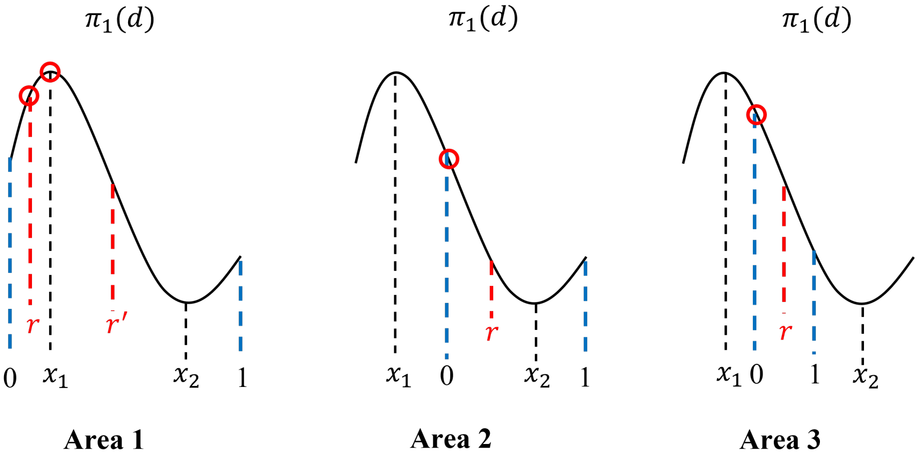
$$\begin{aligned}
x_2 &\ge 0\\
x_1 &< 1\\
\pi_1^{'}(0) &= \frac{\partial\pi_1(d)}{\partial d}|_{d=0}=\frac{\alpha(3-2c)-1}{2}\\
\pi_1^{'}(1) &= \frac{\partial\pi_1(d)}{\partial d}|_{d=1}=\frac{\alpha(1+2c)-1}{2}\\
\pi_1(0) &= \frac{1-\alpha}{2}>\pi_1(1)=0
\end{aligned}$$

Figure B.4: Case (1a)



	$\pi_1'(0)$	$\pi_1'(1)$		π_{1max}
Area 1	+	+	$0 \leq x_1 < x_2 < 1$	$\pi(1 - c - min\{r - \epsilon,\ x_1\},\ min\{r - \epsilon,\ x_1\})$
Area 2	-	+	$x_1 \leq 0 < x_2 < 1$	$\pi(1 - c,\ 0)$
Area 3	-	-	$x_1 \leq 0 < 1 < x_2$	$\pi(1 - c,\ 0)$

Figure B.5: Case (1a) Solution



Thus, when $0 \leq \alpha \leq c \leq 1$ and $0 \leq d < r$, the sub-optimal solution is:

$$\widetilde{\pi}^s(\widetilde{P}^s_{out},\ \widetilde{d}^s) = \begin{cases} \pi(1 - c - min\{r - \epsilon,\ x_1\},\ min\{r - \epsilon,\ x_1\}), & \text{for } (\alpha,\ c) \text{ in Area 1} \\ \pi(1 - c,\ 0), \quad \text{for } (\alpha,\ c) \text{ in Areas 2 and 3} \end{cases}$$

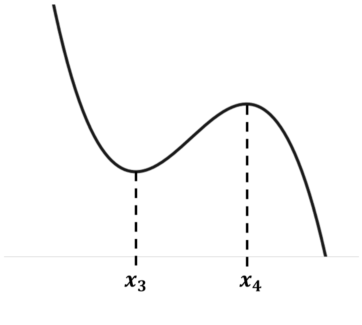
(b) when $0 \leq c < \alpha \leq 1$ and $0 \leq r \leq \dfrac{\alpha - c}{1+\alpha}$, we have:

$$
\begin{aligned}
\widetilde{P}^{s}_{out} &= \frac{1-\alpha c}{1+\alpha} \\
\pi_2(d) &= \left\{ \frac{\alpha(1-\alpha c)(\alpha - c)}{(1+\alpha)^2} + (1-\alpha)\left[\frac{1}{2}\left(\frac{1+c}{1+\alpha} + d \right)^2 + \frac{1-\alpha c}{1+\alpha}\left(\frac{\alpha - c}{1+\alpha} - d \right) \right] \right\} (1-d) \\
&= -\frac{1-\alpha}{2} d^3 + \frac{(1-\alpha)(1-2c)}{2} d^2 + \frac{2\alpha c(1-\alpha) - (1-c)^2}{2(1+\alpha)} d + \frac{c^2 - 2\alpha c + 1}{2(1+\alpha)} \\
\pi_2'(d) &= -\frac{3(1-\alpha)}{2} d^2 + (1-\alpha)(1-2c) d + \frac{2\alpha c(1-\alpha) - (1-c)^2}{2(1+\alpha)} \\
\Delta_2 &= \left[(1-\alpha)(1-2c)\right]^2 + \frac{3(1-\alpha)\left[2\alpha c(1-\alpha) - (1-c)^2\right]}{1+\alpha} \\
&= \frac{1-\alpha}{1+\alpha}\left[(1-\alpha^2)(1-2c)^2 + 6\alpha c(1-\alpha) - 3(1-c)^2\right]
\end{aligned}
$$

In area 5, we have $\Delta_2 < 0$. Thus, $\pi_2(d)$ is decreasing in d.

In area 4, we have $\Delta_2 > 0$. Thus, $\pi_2(d)$ is a cubic function with two extremum points (x_3, x_4). Figure B.6 provides an illustration of such cubic function.

Figure B.6: Illustration of Cubic Profit Function 2



$$
\begin{aligned}
x_3 &= \frac{(1-\alpha)(1-2c) - \sqrt{\Delta_2}}{3(1-\alpha)} \\
x_4 &= \frac{(1-\alpha)(1-2c) + \sqrt{\Delta_2}}{3(1-\alpha)}
\end{aligned}
$$

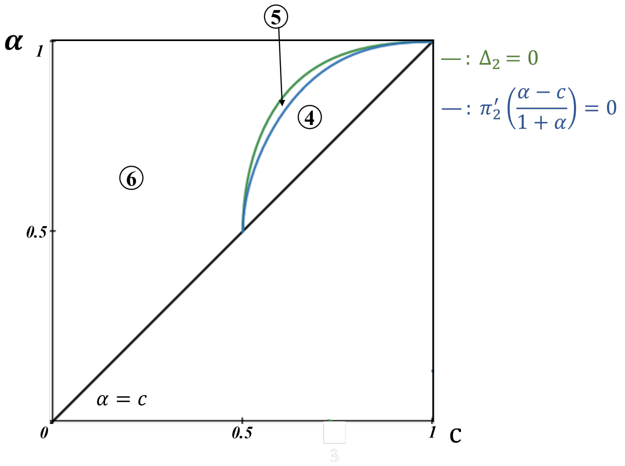
Notice that,

$$\begin{aligned}
\pi_2^{'}(0) &= \frac{2\alpha c(1-\alpha)-(1-c)^2}{2(1+\alpha)} > 0 \quad \text{for } (\alpha,\ c) \text{ in Area 4} \\
\pi_2^{'}(1) &= \frac{(1+2c)\alpha^2+2\alpha c-c^2-2c-2}{2(1+\alpha)} < 0 \quad \text{for } (\alpha,\ c) \text{ in Area 4} \\
\pi_2^{'}\left(\frac{\alpha-c}{1+\alpha}\right) &= \frac{(1+2c)\alpha^3-(3+4c+4c^2)\alpha^2+(1+6c+2c^2)\alpha-1}{2(1+\alpha)^2} \\
\frac{x_3+x_4}{2} &= \frac{1-2c}{3} \leq \frac{\alpha-c}{1+\alpha} \quad \text{for } \frac{1}{2} \leq \alpha \leq 1
\end{aligned}$$

Therefore, we have:

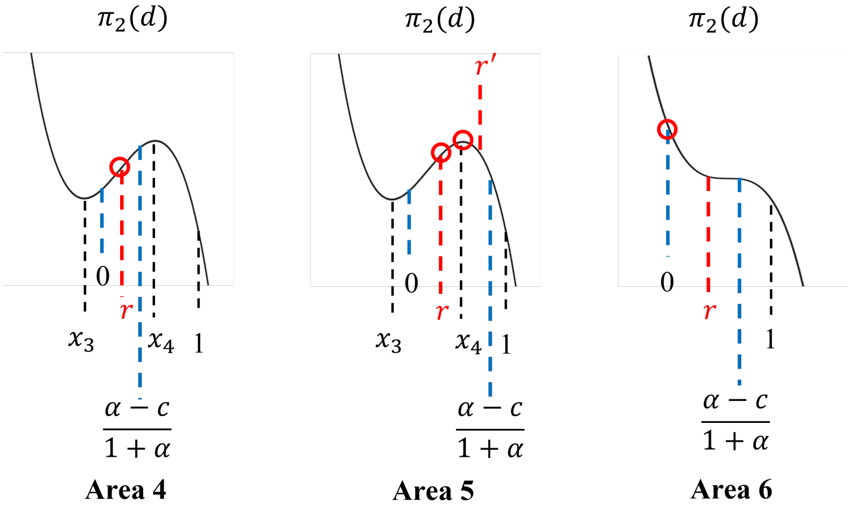
$$x_3 < 0 < r < \frac{\alpha-c}{1+\alpha} < x_4 < 1$$

Figure B.7: Case (1b)



	$\pi_2^{'}(0)$	$\pi_2^{'}\left(\frac{\alpha-c}{1+\alpha}\right)$		π_{2max}
Area 4	+	+	$x_3 < 0 < r \leq \frac{\alpha-c}{1+\alpha} < x_4 < 1$	$\pi\left(\frac{1-\alpha c}{1+\alpha},\ r-\epsilon\right)$
Area 5	+	-	$x_3 < 0 < x_4 < \frac{\alpha-c}{1+\alpha} < 1$	$\pi\left(\frac{1-\alpha c}{1+\alpha},\ min\{x_4,\ r-\epsilon\}\right)$
Area 6	-	-	$\pi_2(d)$ is decreasing in d	$\pi\left(\frac{1-\alpha c}{1+\alpha},\ 0\right)$

Figure B.8: Case (1b) Solution



Thus, when $0 \leq c < \alpha \leq 1$ and $0 \leq d < r \leq \dfrac{\alpha - c}{1+\alpha}$, the sub-optimal solution is:

$$\widetilde{\pi}^s(\widetilde{P}^s_{out},\ \widetilde{d}^s) = \begin{cases} \pi\left(\dfrac{1-\alpha c}{1+\alpha},\ r-\epsilon\right), & \text{for } (\alpha,\ c) \text{ in Area 4} \\ \pi\left(\dfrac{1-\alpha c}{1+\alpha},\ min\{x_4,\ r-\epsilon\}\right), & \text{for } (\alpha,\ c) \text{ in Area 5} \\ \pi\left(\dfrac{1-\alpha c}{1+\alpha},\ 0\right), & \text{for } (\alpha,\ c) \text{ in Area 6} \end{cases}$$

(c) When $0 \leq c < \alpha \leq 1$ and $(\alpha - c)/(1+\alpha) < r \leq 1$, we have:

$$\pi(d) = \begin{cases} \pi_2(d), & \text{if} \quad 0 \leq d < \dfrac{\alpha-c}{1+\alpha} \\ \pi_1(d), & \text{if} \quad \dfrac{\alpha-c}{1+\alpha} \leq d < r \end{cases}$$

We need to identify the shape of $\pi_2(d)$ in $\left[0, \dfrac{\alpha-c}{1+\alpha}\right)$ and the shape of $\pi_1(d)$ in $\left[\dfrac{\alpha-c}{1+\alpha}, 1\right)$.

Notice that:

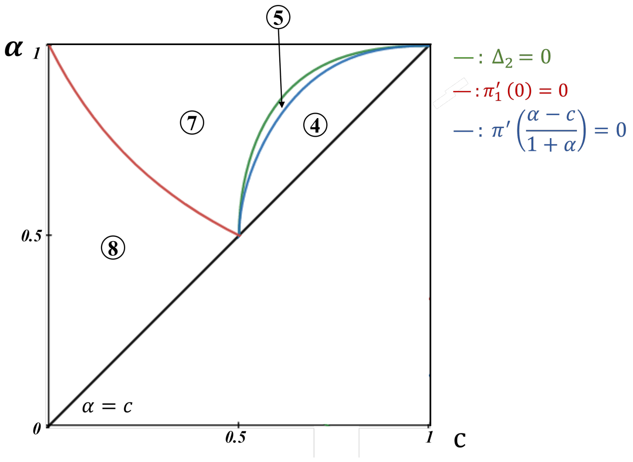
$$\pi_1\left(\frac{\alpha-c}{1+\alpha}\right) = \pi_2\left(\frac{\alpha-c}{1+\alpha}\right) = \pi\left(\frac{1-\alpha c}{1+\alpha},\ \frac{\alpha-c}{1+\alpha}\right)$$

$$\pi_1'\left(\frac{\alpha-c}{1+\alpha}\right) = \pi_2'\left(\frac{\alpha-c}{1+\alpha}\right)$$

$$\frac{x_1+x_2}{2} = \frac{2-c}{3} > \frac{\alpha-c}{1+\alpha} \quad \text{for any } (\alpha,\ c) \text{ in } (0,\ 1) \times (0,\ 1)$$

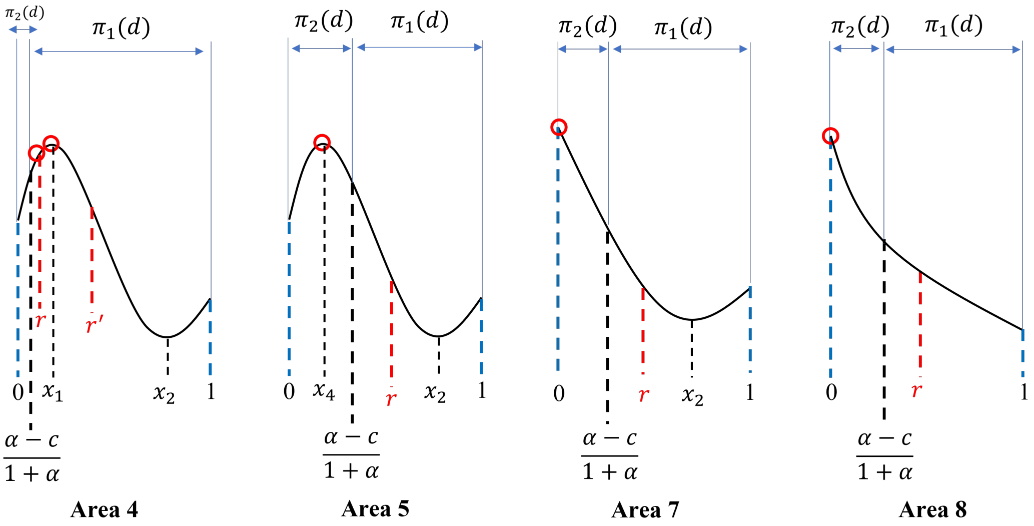
$$x_1 < 1$$

Figure B.9: Case (1c)



	$\pi_2^{'}(0)$	$\pi^{'}(\frac{\alpha-c}{1+\alpha})$	$\pi_1^{'}(1)$	π_{max}
Area 4	+	+	+	$\pi\,(1 - c - min\{x_1,\ r-\epsilon\},\ min\{x_1,\ r-\epsilon\})$
Area 5	+	-	+	$\pi\left(\frac{\alpha-c}{1+\alpha},\ x_4\right)$
Area 7	-	-	+	$\pi\left(\frac{1-\alpha c}{1+\alpha},\ 0\right)$
Area 8	-	-	-	$\pi\left(\frac{1-\alpha c}{1+\alpha},\ 0\right)$

Figure B.10: Case (1b) Solution



Thus, when $0 \leq c < \alpha \leq 1$ and $\dfrac{\alpha - c}{1+\alpha} < r \leq 1$, the sub-optimal solution is:

$$\widetilde{\pi}^s(\widetilde{P}^s_{out},\ \widetilde{d}^s) = \begin{cases} \pi\left(1 - c - min\{x_1,\ r-\epsilon\},\ min\{x_1,\ r-\epsilon\}\right), & \text{for } (\alpha,\ c) \text{ in Area 4} \\ \pi\left(\dfrac{1-\alpha c}{1+\alpha},\ x_4\right), & \text{for } (\alpha,\ c) \text{ in Area 5} \\ \pi\left(\dfrac{1-\alpha c}{1+\alpha},\ 0\right), & \text{for } (\alpha,\ c) \text{ in Areas 7 and 8} \end{cases}$$

(2) $1 - c - d < P_{out} \leq 1 - c$

In this case, the seller faces the following profit function:

$$\pi(P_{out}, d) = \left[\underbrace{\alpha P_{out}(1 - P_{out} - c)}_{\text{Profit from } S \text{ users}} + \underbrace{(1-\alpha)\int_0^1 v dv}_{\text{Profit from } NS \text{ users}}\right](1-d)$$

We have:

$$\widetilde{P}_{out} = \max\left\{1 - c - d,\quad \frac{1-c}{2}\right\}$$

(a) When $0 \leq r \leq \dfrac{1-c}{2}$, $1 - c - d > \dfrac{1-c}{2}$; we have:

$$\begin{aligned} \widetilde{P}_{out} &= 1 - c - d \\ \pi_1(d) &= \left[\alpha(1-c-d)d + \frac{1-\alpha}{2}\right](1-d) \end{aligned}$$

According to the proof of case (1a), we need to figure out the relationship between 0, r, $\dfrac{1-c}{2}$, x_1 and x_2.

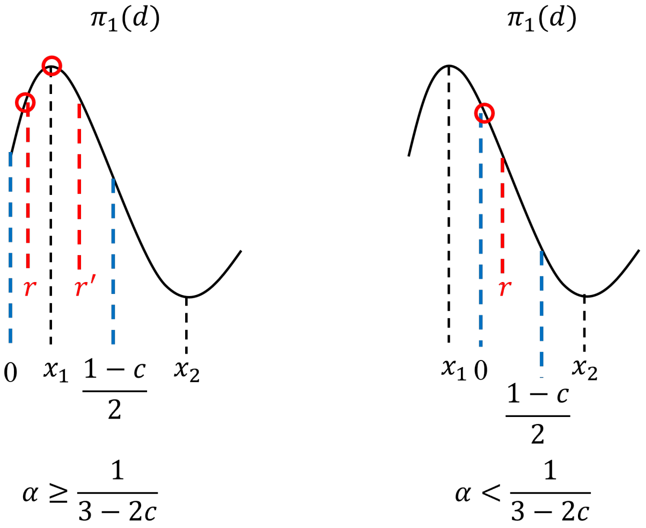
Notice that:

$$\begin{aligned} \pi_1^{'}\left(\frac{1-c}{2}\right) &= \frac{\alpha(1+2c-c^2)-2}{4} < 0 \text{ for any } (\alpha,\ c) \text{ in } (0,\ 1)\times(0\ ,1). \\ \pi_1^{'}(0) &= \frac{\alpha(3-2c)-1}{2} \\ \frac{1-c}{2} &< \frac{2-c}{3} = \frac{x_1 + x2}{2} < x_2 \end{aligned}$$

Thus, we have:

$$\begin{cases} 0 \leq x_1 < \dfrac{1-c}{2} < x_2, & \text{if } \alpha \geq \dfrac{1}{3-2c} \\ x_1 < 0 < r < \dfrac{1-c}{2} < x_2, & \text{otherwise} \end{cases}$$

Figure B.11: Case (2a) Solution



Thus, when $0 \leq d < r \leq (1-c)/2$ and $1-c-d < P_{out} \leq 1-c$, the sub-optimal solution is:

$$\widetilde{\pi}^s(\widetilde{P}_{out}^s,\ \widetilde{d}^s) = \begin{cases} \pi(1-c,0), & \text{if } \alpha < \dfrac{1}{3-2c} \\ \pi(1-c-min\left\{r-\epsilon, x_1\right\}, min\left\{r-\epsilon, x_1\right\}), & \text{otherwise} \end{cases}$$

(b) When $r > \dfrac{1-c}{2}$, we have:

$$\pi(d) = \begin{cases} \left[\alpha(1-c-d)d + \dfrac{1-\alpha}{2}\right](1-d), & \text{if } \quad 0 \leq d < \dfrac{1-c}{2} \\ \left[\alpha\left(\dfrac{1-c}{2}\right)^2 + \dfrac{1-\alpha}{2}\right](1-d), & \text{if } \quad \dfrac{1-c}{2} \leq d < r \end{cases}$$

When $\dfrac{1-c}{2} \leq d < r$, $\pi(d)$ is decreasing in d. The sub-optimal point will not exceed $\dfrac{1-c}{2}$, therefore, the solution of case (2b) is the same as case (2a).

Combining the results of case (2a) and (2b), when $0 \leq d < r$ and $1-c-d < P_{out} \leq 1-c$, the sub-optimal solution is:

$$\widetilde{\pi}^s(\widetilde{P}_{out}^s,\ \widetilde{d}^s) = \begin{cases} \pi(1-c,0), & \text{if } \alpha < \dfrac{1}{3-2c} \\ \pi(1-c-min\left\{r-\epsilon, x_1\right\}, min\left\{r-\epsilon, x_1\right\}), & \text{otherwise} \end{cases}$$

(3) $1-c < P_{out}$

In this case, all privacy sensitive (S) users choose to opt-out and not buy while all privacy non-sensitive (NS) users choose to opt-in and buy. The seller's profit is:

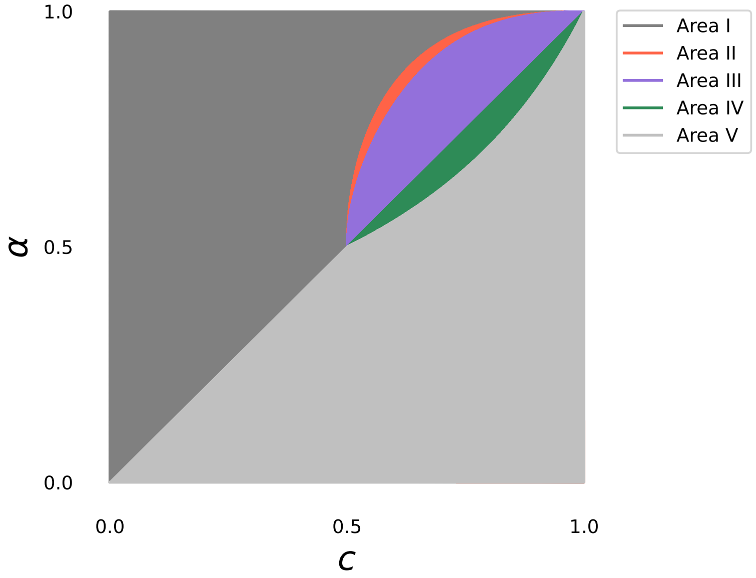
$$\pi(d) = \left[(1-\alpha)\int_0^1 v dv\right](1-d) = \frac{(1-\alpha)(1-d)}{2}$$

It is decreasing in d. Thus, the sub-optimal solution is:

$$\widetilde{\pi}^s(\widetilde{P}^s_{out},\ \widetilde{d}^s) = \pi(\overline{P}_{out},\ 0)$$
$$\text{where } \overline{P}_{out} > 1-c$$

To sum up, when $0 \leq d < r$, the sub-optimal (P^s_{out}, d^s) combination is presented in Figure B.12.

Figure B.12: Solution for $0 \leq d < r$ and $\lambda = 1$



For (α, c) in:

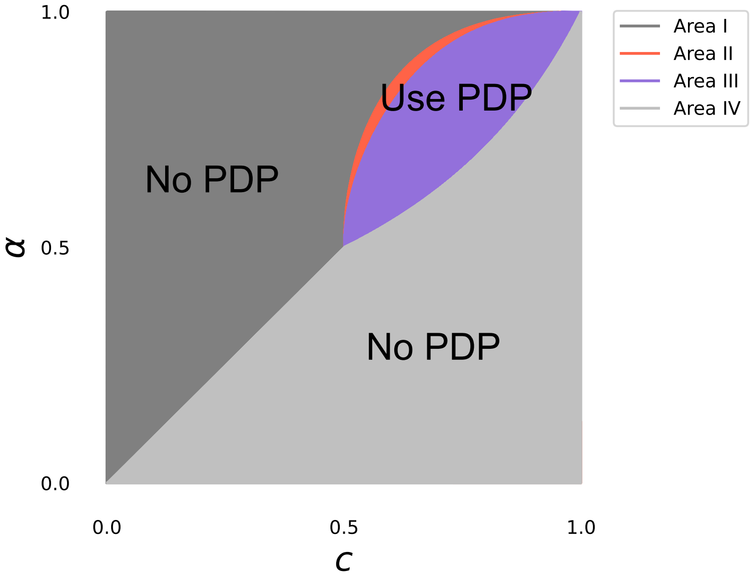
- Area I: $(\widetilde{P}^s_{out},\ \widetilde{d}^s) = \left(\frac{1-\alpha c}{1+\alpha},\ 0\right)$
- Area II: $(\widetilde{P}^s_{out},\ \widetilde{d}^s) = \left(\frac{1-\alpha c}{1+\alpha},\ min\{x_4,\ r-\epsilon\}\right)$
- Area III: $(\widetilde{P}^s_{out},\ \widetilde{d}^s) = \begin{cases} \left(\frac{1-\alpha c}{1+\alpha},\ r-\epsilon\right), & \text{if } 0 \leq r \leq \frac{\alpha - c}{1+\alpha} \\ (1-c-min\{x_1,\ r-\epsilon\},\ min\{x_1,\ r-\epsilon\}), & \text{otherwise} \end{cases}$
- Area IV: $(\widetilde{P}^s_{out},\ \widetilde{d}^s) = (1-c-min\{x_1,\ r-\epsilon\},\ min\{x_1,\ r-\epsilon\})$

- Area V: $(\widetilde{P}^s_{out},\ \widetilde{d}^s) = (1-c,\ 0)$

At last, let us compare the sub-optimal solution from $0 \leq d < r$ and the sub-optimal solution from $d \geq r$ to figure out the global optimal strategy and profit.

Notice that, the strategy $(P_{out}, r-\epsilon)$ is always dominated by the strategy (P_{out}, r) since a small increase of d by ϵ will seldom increase the market shrink effect $(1-d)$ while it will dramatically increase the opt-in market by making low valuation privacy sensitive (S) users who are used to be not covered by the market choose to opt-in and buy the product.

Figure B.13: Global Solution for $\lambda = 1$



Taken together, the global equilibrium is:

For (α, c) in:

- Area I: $(P^{s*}_{out1},\ d^{s*}_1) = \begin{cases} (\overline{P}_{out},\ r), & \text{if} \quad 0 \leq r \leq r_1 \\ \left(\dfrac{1-\alpha c}{1+\alpha},\ 0\right), & \text{if} \quad r_1 < r \leq 1 \end{cases}$

- Area II: $(P^{s*}_{out2},\ d^{s*}_2) = \begin{cases} (\overline{P}_{out},\ r), & \text{if} \quad 0 \leq r \leq r_2 \\ \left(\dfrac{1-\alpha c}{1+\alpha},\ x_4\right), & \text{if} \quad r_2 < r \leq 1 \end{cases}$

- Area III: $(P^{s*}_{out3},\ d^{s*}_3) = \begin{cases} (\overline{P}_{out},\ r), & \text{if } 0 \leq r \leq r_3 \\ (1-c-x_1,\ x_1), & \text{if } r_3 < r \leq 1 \end{cases}$

- Area IV: $(P^{s*}_{out4},\ d^{s*}_{4}) = \begin{cases} (\overline{P}_{out},\ r), & \text{if } 0 \leq r \leq \alpha \\ (\overline{P}_{out},\ 0), & \text{if } \alpha < r \leq 1 \end{cases}$

where

- $r_1 = \dfrac{(1+2c)\alpha - c^2}{1+\alpha}$
- $r_2 = max\left\{x_4,\ 1 - 2\pi\left(\dfrac{1-\alpha c}{1+\alpha},\ x_4\right)\right\}$
- $r_3 = max\left\{x_1,\ 1 - 2\pi(1-c-x_1,\ x_1)\right\}$
- $x_1 = \dfrac{2\alpha(2-c) - \sqrt{[2\alpha(2-c)]^2 - 6\alpha(3\alpha - 2\alpha c - 1)}}{6\alpha}$
- $x_4 = \dfrac{(1-\alpha)(1-2c) + \sqrt{\frac{1-\alpha}{1+\alpha}\left[(1-\alpha^2)(1-2c)^2 + 6\alpha c(1-\alpha) - 3(1-c)^2\right]}}{3(1-\alpha)}$
- $\overline{P}_{out} \geq 1 - c$

B.4 Proof of Lemma 4, 5 and 6

1. Low r, for $(\alpha,\ c)$ in $(0,\ 1) \times (0,\ 1)$:

$$\begin{aligned} (P^{s*}_{in}(v),\ P^{s*}_{out},\ d^{s*}) &= (v,\ \overline{P}_{out},\ r),\ where\ \overline{P}_{out} \geq 1 - c \\ CS^{s*} &= (1-d^{s*})[-\alpha r + (1-\alpha) * 0] - (d^{s*})^2 = -\alpha r + (\alpha - 1)r^2 \\ \pi^{s*} &= \frac{1-r}{2} \\ TW^{s*} &= CS^{s*} + \pi^{s*} = \frac{1 - (1+2\alpha)r + 2(\alpha-1)r^2}{2} \end{aligned}$$

2. High r, for $(\alpha,\ c)$ in:

(1) Area I

$$\begin{aligned} (P^{s*}_{in}(v),\ P^{s*}_{out},\ d^{s*}) &= (v,\ \frac{1-\alpha c}{1+\alpha},\ 0) \\ CS^{s*} &= \int_{\frac{1+c}{1+\alpha}}^{1} \left(v - \frac{1+c}{1+\alpha}\right) dv = \frac{(\alpha - c)^2}{2(1+\alpha)^2} \\ \pi^{s*} &= (1-\alpha)\int_0^{\frac{1+c}{1+\alpha}} v dv + \frac{1-\alpha c}{1+\alpha}\left(1 - \frac{1+c}{1+\alpha}\right) = \frac{1 + c^2 - 2\alpha c}{2(1+\alpha)} \\ TW^{s*} &= CS^{s*} + \pi^{s*} = \frac{(\alpha - c)^2 + (1 + c^2 - 2\alpha c)(1+\alpha)}{2(1+\alpha)^2} \end{aligned}$$

For α, we have:

$$\begin{aligned}
\frac{\partial CS^{s*}}{\partial\alpha} &= \frac{(\alpha-c)(1+c)}{(1+\alpha)^3} \geq 0 \\
\frac{\partial\pi^{s*}}{\partial\alpha} &= -\frac{(1+c)^2}{2(1+\alpha)^2} < 0 \\
\frac{\partial TW^{s*}}{\partial\alpha} &= \frac{(1+c)[(\alpha-1)-(3+\alpha)c)]}{2(1+\alpha)^3} \leq 0
\end{aligned}$$

For c, we have:

$$\begin{aligned}
\frac{\partial CS^{s*}}{\partial c} &= \frac{c-\alpha}{(1+\alpha)^2} \leq 0 \\
\frac{\partial\pi^{s*}}{\partial c} &= \frac{c-\alpha}{1+\alpha} \leq 0 \\
\frac{\partial TW^{s*}}{\partial c} &= \frac{(2+\alpha)(c-\alpha)}{(1+\alpha)^2} \leq 0
\end{aligned}$$

(2) Area II

$$\begin{aligned}
&(P^{s*}_{in}(v),\ P^{s*}_{out},\ d^{s*}) = (v,\ \frac{1-\alpha c}{1+\alpha},\ x_4) \\
&CS^{s*} = -x_4^2 + \alpha(1-x_4)\left(-\frac{(1+c)x_4}{1+a} + \int_{\frac{1+c}{1+\alpha}}^{1}\left(v-\frac{1+c}{1+\alpha}-x_4\right)dv\right) \\
&\qquad + (1-\alpha)(1-x_4)\int_{\frac{1+c}{1+\alpha}+x_4}^{1}\left(v-\frac{1+c}{1+\alpha}-x_4\right)dv \\
&\pi^{s*} = \left\{\frac{\alpha(1-\alpha c)(\alpha-c)}{(1+\alpha)^2} + (1-\alpha)\left[\int_0^{\frac{1+c}{1+\alpha}+x_4} vdv + \frac{1-\alpha c}{1+\alpha}\left(\frac{\alpha-c}{1+\alpha}-x_4\right)\right]\right\}(1-x_4) \\
&TW^{s*} = CS^{s*} + \pi^{s*}
\end{aligned}$$

where,

$$x_4 = \frac{(1-\alpha)(1-2c) + \sqrt{\frac{1-\alpha}{1+\alpha}\left[(1-\alpha^2)(1-2c)^2 + 6\alpha c(1-\alpha) - 3(1-c)^2\right]}}{3(1-\alpha)}$$

Due to the complex function of $x_4(\alpha, c)$, $CS(\alpha, c)$ and $\pi(\alpha, c)$, it is difficult to figure out the sign of their derivative w.r.t α and c. In this section, we use numerical analysis method to conduct static comparative analysis.

Figure B.14: Welfare Analysis in Area II w.r.t α

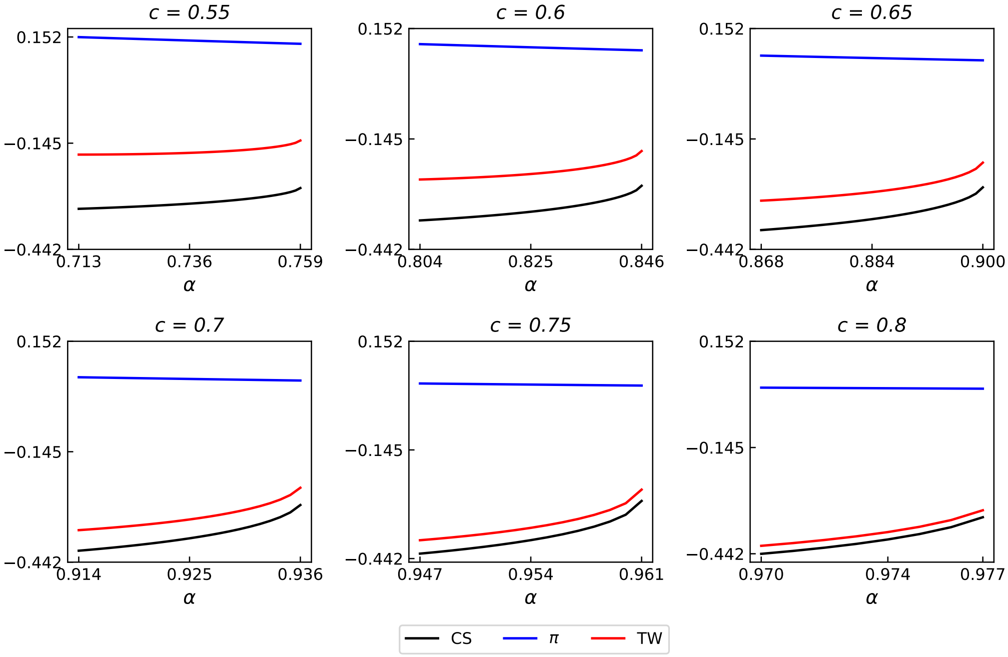
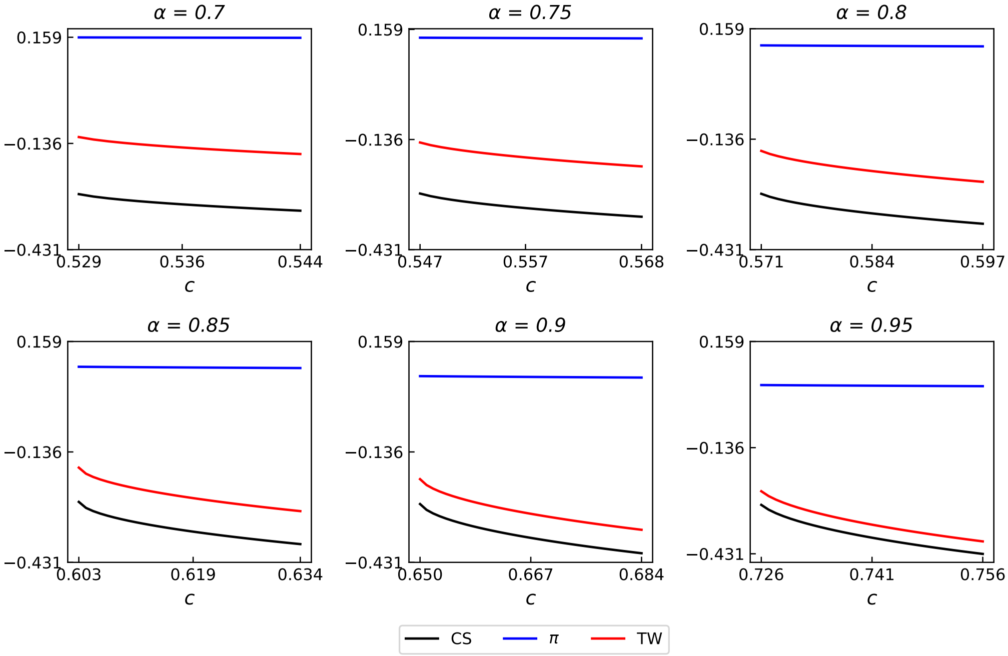


Figure B.15: Welfare Analysis in Area II w.r.t c



(3) Area III

$$
\begin{aligned}
(P^{s*}_{in}(v),\ P^{s*}_{out},\ d^{s*}) &= (v,\ 1-c-x_1,\ x_1)\\
CS^{s*} &= -x_1^2 + \alpha(1-x_1)\left[-x_1(1-x_1) + \int_{1-x_1}^{1}(v-1)dv\right]\\
\pi^{s*} &= \alpha(1-x_1)(1-c-x_1)x_1 + (1-\alpha)(1-x_1)\int_0^1 vdv\\
TW^{s*} &= CS^{s*} + \pi^{s*}
\end{aligned}
$$

where,

$$x_1 = \frac{2\alpha(2-c) - \sqrt{[2\alpha(2-c)]^2 - 6\alpha(3\alpha - 2\alpha c - 1)}}{6\alpha}$$

Figure B.16: Welfare Analysis in Area III w.r.t α

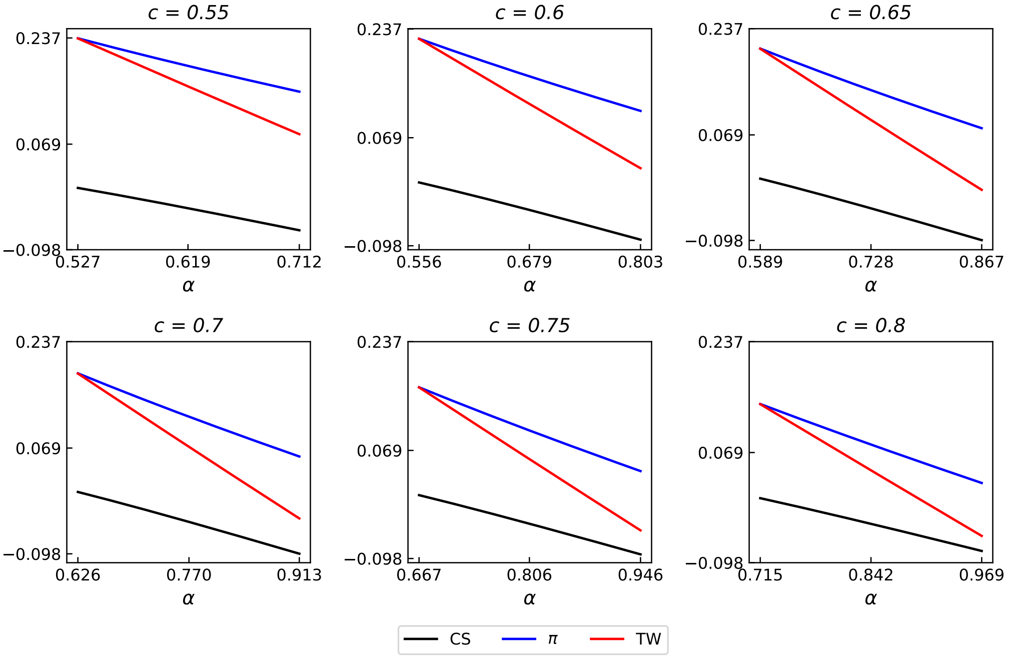
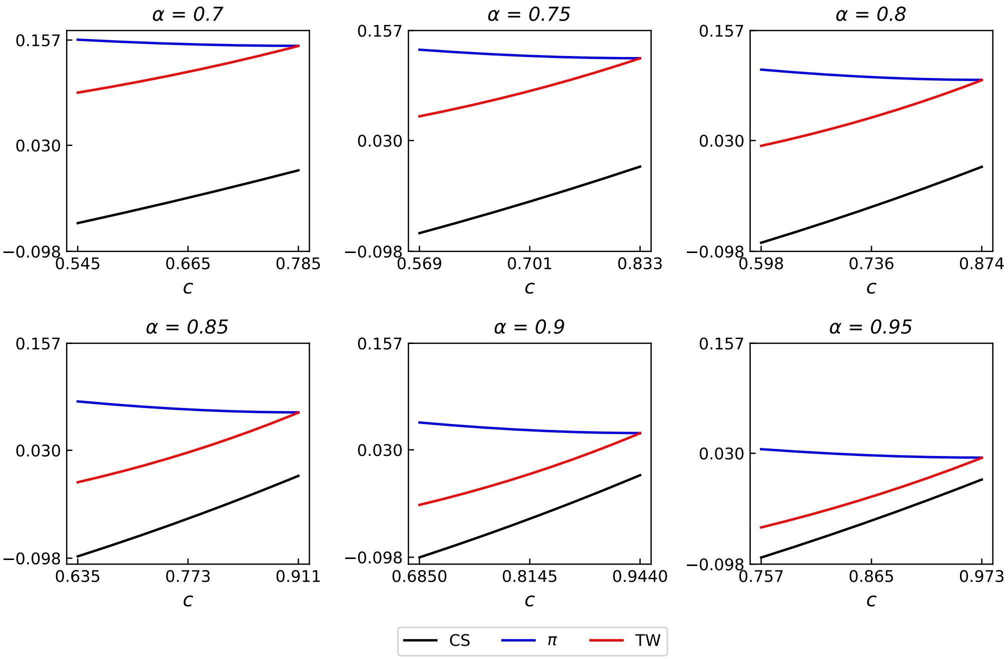


Figure B.17: Welfare Analysis in Area III w.r.t c



(4) Area IV

$$(P_{in}^{s*}(v),\ P_{out}^{s*},\ d^{s*}) = (v,\ 1-c,\ 0)$$

$$CS^{s*} = 0$$

$$\pi^{s*} = \frac{1-\alpha}{2}$$

$$TW^{s*} = CS^{s*} + \pi^{s*} = \frac{1-\alpha}{2}$$

B.5 Proof of Proposition 1

In the benchmark model, we have:

$$CS^{b*} = \begin{cases} \dfrac{(\alpha - c)^2}{2(1+\alpha)^2}, & 0 \leq c \leq \alpha \leq 1 \\ 0, & 0 \leq \alpha < c \leq 1 \end{cases}$$
$$\pi^{b*} = \begin{cases} \dfrac{1 + c^2 - 2\alpha c}{2(1+\alpha)}, & 0 \leq c \leq \alpha \leq 1 \\ \dfrac{1-\alpha}{2}, & 0 \leq \alpha < c \leq 1 \end{cases}$$
$$TW^{b*} = \begin{cases} \dfrac{(\alpha - c)^2 + (1 + c^2 - 2\alpha c)(1+\alpha)}{2(1+\alpha)^2}, & 0 \leq c \leq \alpha \leq 1 \\ \dfrac{1-\alpha}{2}, & 0 \leq \alpha < c \leq 1 \end{cases}$$

In the naïve users model, we have:

$$CS^{n*} = -\alpha r$$
$$\pi^{n*} = \frac{1}{2}$$
$$TW^{n*} = \frac{1}{2} - \alpha r$$

Obviously, we have:

$$CS^{b*} \geq CS^{n*}$$
$$\pi^{b*} \leq \pi^{n*}$$
$$\begin{cases} TW^{b*} \geq TW^{n*}, & \text{if } r \geq \overline{r} \\ TW^{b*} < TW^{n*}, & \text{otherwise} \end{cases}$$

where

$$\overline{r} = \begin{cases} \dfrac{(1+\alpha)(\alpha - c^2 + 2\alpha c) - (\alpha - c)^2}{2\alpha(1+\alpha)^2} \in (0,1), & \text{if } 0 \leq c \leq \alpha \leq 1 \\ \dfrac{1}{2}, \quad \text{if } 0 \leq \alpha < c \leq 1 \end{cases}$$

According to the proof of previous section, we have:

$(\alpha,\ c)$	r	$CS^{s*} - CS^{b*}$	$\pi^{s*} - \pi^{b*}$	$TW^{s*} - TW^{b*}$
Area I	$[0, r_1]$	-	+	- or +
	$(r_1, 1]$	0	0	0
Area II	$[0, r_2]$	-	+	- or +
	$(r_2, 1]$	-	+	- or +
Area III	$[0, r_3]$	-	+	- or +
	$(r_3, 1]$	-	+	- or +
Area IV	$[0, \alpha]$	-	+	- or +
	$(\alpha, 1]$	0	0	0

Table B.1: Comparison between Benchmark and Sophisticated Users Model

B.6 Proof of Proposition 2

In this section, we consider a social planner who aims to maximize total social welfare. In stage 1, the social planner will set a PDP level d rather than the seller. For instance, the social planner regulates the PDP practices. The analysis is similar to the proof lemma 3 while the objective function is total social welfare rather than the seller's profit.

Case 1: $d \geq r$

Given $d \geq r$, the sellers will choose $P_{out} \geq 1 - c$, the total social welfare is:

$$\begin{aligned} TW(d) &= CS(d) + \pi(d) \\ &= d * (-d) + (1-d) * [\alpha * (-r) + (1-\alpha) * 0] + \frac{1-d}{2} \\ &= \frac{-2d^2 + (2\alpha r - 1)d + 1 - 2\alpha r}{2} \\ d^{w*} &= max\left\{r,\ \frac{2\alpha r - 1}{4}\right\} = r \\ TW^{w*} &= \frac{2(\alpha-1)r^2 - (1+2\alpha)r + 1}{2} \end{aligned}$$

Case 2: $0 \leq d < r$

(1) $0 \leq P_{out} \leq 1 - c - d$

(a) When $0 \leq \alpha \leq c \leq 1$, we have:

$$\begin{aligned}
\widetilde{P}_{out} &= 1 - c - d \\
\pi_1(d) &= \left[\alpha(1 - c - d)d + (1 - \alpha)\int_0^1 v dv\right](1 - d) \\
CS_1(d) &= -d^2 + \alpha(1 - d)[-d(1 - d) + \int_{1-d}^1 (v - 1)dv] \\
TW_1(d) &= CS_1(d) + \pi_1(d) \\
&= \frac{\alpha d^3 + (2\alpha c - \alpha - 2)d^2 - (2\alpha c - \alpha + 1)d + 1 - \alpha}{2} \\
\frac{\partial TW_1(d)}{\partial d} &= \frac{3\alpha d^2 + 2(2\alpha c - \alpha - 2)d - (2\alpha c - \alpha + 1)}{2} \\
\Delta_1 &= 2(2c^2 + c - 1)\alpha^2 + (7 - 8c)\alpha + 4 > 0
\end{aligned}$$

Thus, $TW_1(d)$ is a cubic function of d which has two extremum points $(x_1,\ x_2)$ (Figure B.3).

$$\begin{aligned}
x_1 &= \frac{\alpha(2c - 1) - 2 - \sqrt{\Delta_1}}{3\alpha} \\
x_2 &= \frac{\alpha(2c - 1) - 2 + \sqrt{\Delta_1}}{3\alpha}
\end{aligned}$$

Notice that:

$$\begin{aligned}
TW_1^{'}(0) &= \frac{\alpha(1 - 2c) - 1}{2} < 0 \\
TW_1^{'}(1) &= \alpha(c + 1) - \frac{5}{2} < 0 \\
TW_1(0) &= \frac{1 - \alpha}{2} > TW_1(1) = -1
\end{aligned}$$

Thus, $TW_1(d)$ is a decreasing function in $[0, 1]$. Therefore, when $0 \leq \alpha \leq c \leq 1$ and $0 \leq d < r$, the sub-optimal solution is:

$$\widetilde{TW}^w(\widetilde{P}_{out}^w,\ \widetilde{d}^w) = TW_1(0)$$

(b) When $0 \leq c < \alpha \leq 1$ and $0 \leq r \leq (\alpha - c)/(1+\alpha)$, we have:

$$
\begin{aligned}
\widetilde{P}^{s}_{out} &= \frac{1-\alpha c}{1+\alpha} \\
\pi_2(d) &= \left\{ \frac{\alpha(1-\alpha c)(\alpha - c)}{(1+\alpha)^2} + (1-\alpha)\left[\frac{1}{2}\left(\frac{1+c}{1+\alpha} + d\right)^2 + \frac{1-\alpha c}{1+\alpha}\left(\frac{\alpha - c}{1+\alpha} - d\right)\right]\right\}(1-d) \\
CS_2(d) &= -d^2 + \alpha(1-d)\left(-\frac{(1+c)d}{1+a} + \int_{\frac{1+c}{1+\alpha}}^{1}\left(v - \frac{1-\alpha c}{1+\alpha} - c - d\right)dv\right) \\
&\quad + (1-\alpha)(1-d)\int_{\frac{1+c}{1+\alpha}+d}^{1}\left(v - \frac{1-\alpha c}{1+\alpha} - c - d\right)dv \\
TW_2(d) &= CS_2(d) + \pi_2(d) \\
&= (\alpha - 1)d^3 + \frac{(\alpha-1)[\alpha(c-1)+2c]}{1+\alpha}d^2 \\
&\quad - \frac{2c\alpha^3 + (2c+5)\alpha^2 + (c^2 - 6c + 5)\alpha + 2c^2 - 4c + 1}{2(1+\alpha)^2}d \\
&\quad + \frac{(1-2c)\alpha^2 + (c^2 - 4c + 1)\alpha + 2c^2 + 1}{2(1+\alpha)^2} \\
TW_2^{'}(d) &= 3(\alpha - 1)d^2 + \frac{2(\alpha-1)[\alpha(c-1)+2c]}{1+\alpha}d \\
&\quad - \frac{2c\alpha^3 + (2c+5)\alpha^2 + (c^2 - 6c + 5)\alpha + 2c^2 - 4c + 1}{2(1+\alpha)^2} \\
\Delta_2 &= \frac{2(\alpha - 1)\left[2\alpha^3(1+c+c^2) + \alpha^2(13 + 2c + 6c^2) + \alpha(15 - 10c + 3c^2) + 3 - 12c - 2c^2\right]}{(1+\alpha)^2} \\
\Delta_2 &< 0 \\
TW_2^{'}(d) &< 0
\end{aligned}
$$

Thus, $TW_2(d)$ is a decreasing function. Therefore, when $0 \leq c < \alpha \leq 1$ and $0 \leq d < r \leq (\alpha - c)/(1+\alpha)$, the sub-optimal solution is:

$$\widetilde{TW}^{w}(\widetilde{P}^{w}_{out},\ \widetilde{d}^{w}) = TW_2(0)$$

(c) When $0 \leq c < \alpha \leq 1$ and $(\alpha - c)/(1+\alpha) < r \leq 1$, we have:

$$
TW(d) = \begin{cases} TW_2(d), & \text{if} \quad 0 \leq d < \dfrac{\alpha - c}{1+\alpha} \\ TW_1(d), & \text{if} \quad \dfrac{\alpha - c}{1+\alpha} \leq d < r \end{cases}
$$

According to the proof of case (1b), $TW_2(d)$ is decreasing in $\left[0, \dfrac{\alpha - c}{1+\alpha}\right)$. According to the proof of case (1a), $TW_1(d)$ is decreasing in $\left[\dfrac{\alpha - c}{1+\alpha}, 1\right)$.

Therefore, when $0 \leq c < \alpha \leq 1$ and $(\alpha - c)/(1+\alpha) < r \leq 1$, the sub-optimal solution is:

$$\widetilde{TW}^{w}(\widetilde{P}^{w}_{out},\ \widetilde{d}^{w}) = TW_2(0)$$

(2) $1 - c - d < P_{out} \leq 1 - c$

This is a special case of case (1). According to the proof of case (1), this case is always inferior since the sub-optimal P_{out} will never be $1 - c - d$.

(3) $1 - c < P_{out}$

This is a special case of case (2).

Taken together, the sub-optimal solution for $0 \leq d < r$ is:

$$\widetilde{TW}^{w}(\widetilde{P}^{w}_{out},\ \widetilde{d}^{w}) = \begin{cases} TW_1(0), \text{ if } 0 \leq \alpha \leq c \leq 1 \\ TW_2(0), \text{ if } 0 \leq c < \alpha \leq 1 \end{cases}$$

We combine this sub-optimal solution from $0 \leq d < r$ and the sub-optimal solution from $d \geq r$ to figure out the global solution.

$$\begin{aligned} TW_1(0) &= \frac{1-\alpha}{2} \\ TW_2(0) &= \frac{(1-2c)\alpha^2 + (1-4c+c^2)\alpha + 2c^2 + 1}{2(1+\alpha)^2} \\ TW(\overline{P}_{out}, r) &= \frac{2(\alpha-1)r^2 - (1+2\alpha)r + 1}{2} \end{aligned}$$

$$(P^{w*}_{out},\ d^{w*}) = \begin{cases} \left(\dfrac{1-\alpha c}{1+\alpha},\ 0\right), & \text{if } \leq c < \alpha \leq 1 \ and \ r_1 < r \leq 1 \\ (1-c,\ 0), & \text{if } 0 \leq \alpha \leq c \leq 1 \ and \ r_2 < r \leq 1 \\ \left(\overline{P}_{out}, r\right), & \text{otherwise} \end{cases}$$

where

$$\begin{aligned} r_1 &= \frac{(1+2\alpha) - \sqrt{\Delta}}{4(\alpha-1)} \in (0,1) \\ \Delta &= (1+2\alpha)^2 - \frac{8(\alpha-1)(2\alpha^2 c + \alpha(1+4c-c^2) - 2c^2)}{(1+\alpha)^2} \\ r_2 &= \frac{(1+2\alpha) - \sqrt{(1+2\alpha)^2 - 8\alpha(\alpha-1)}}{4(\alpha-1)} \in (0,1) \end{aligned}$$

B.7 Extension - PDP Sensitivity λ

B.7.1 Low PDP Sensitivity ($\lambda = 0.5$)

We replicate our proof of Lemma 3 using $\lambda = 0.5$ rather than 1 in this section.

Case 1: $d \geq r$

Similarly, in this case, the sub-optimal solution is:

$$\begin{aligned} \widetilde{P}^s_{out} &\geq 1 - c \\ \widetilde{d}^s &= r \\ \widetilde{\pi}^s(\overline{P}_{out},\ r) &= \frac{2 - r}{4} \end{aligned}$$

where $\overline{P}_{out} \geq 1 - c$

Case 2: $0 \leq d < r$

(1) $0 \leq P_{out} \leq 1 - c - d$

(a) When $0 \leq \alpha \leq c \leq 1$, we have:

$$\begin{aligned} \widetilde{P}_{out} &= 1 - c - d \\ \pi_1(d) &= \left[\alpha(1 - c - d)d + (1 - \alpha)\int_0^1 vdv\right]\left(1 - \frac{d}{2}\right) \\ &= \frac{\alpha}{2}d^3 - \frac{\alpha(3 - c)}{2}d^2 + \frac{5\alpha - 4\alpha c - 1}{4}d + \frac{1 - \alpha}{2} \\ \frac{\partial \pi_1(d)}{\partial d} &= \frac{3\alpha}{2}d^2 - \alpha(3 - c)d + \frac{5\alpha - 4\alpha c - 1}{4} \\ \Delta_1 &= \frac{2\alpha^2(3 - c)^2 - 3\alpha(5\alpha - 4\alpha c - 1)}{2} = \frac{\alpha(3\alpha + 2\alpha c^2 + 3)}{2} > 0 \\ &\text{for any } (\alpha,\ c) \text{ in } (0,\ 1) \times (0,\ 1) \end{aligned}$$

$\pi_1(d)$ is a cubic function of d which has two extremum points $(x_1,\ x_2)$.

$$\begin{aligned} x_1 &= \frac{\alpha(3 - c) - \sqrt{\Delta_1}}{3\alpha} \\ x_2 &= \frac{\alpha(3 - c) + \sqrt{\Delta_1}}{3\alpha} \end{aligned}$$

Notice that:

$$
\begin{aligned}
x_2 &\geq 0 \\
x_1 &< 1 \\
\pi_1^{'}(0) &= \frac{\partial \pi_1(d)}{\partial d}|_{d=0} = \frac{\alpha(5-4c)-1}{4} \\
\pi_1^{'}(1) &= \frac{\partial \pi_1(d)}{\partial d}|_{d=1} = \frac{-1-\alpha}{4} < 0 \\
\pi_1(0) &= \frac{1-\alpha}{2} > \pi_1(1) = \frac{1-\alpha(1+2c)}{4}
\end{aligned}
$$

Thus, when $0 \leq \alpha \leq c \leq 1$ and $0 \leq d < r$, the sub-optimal solution is:

$$
\widetilde{\pi}^s(\widetilde{P}^s_{out},\ \widetilde{d}^s) = \begin{cases} \pi(1-c-min\{r-\epsilon, x_1\}, min\{r-\epsilon, x_1\}), & \text{if } \alpha > \dfrac{1}{5-4c} \\ \pi(1-c, 0), & \text{otherwise} \end{cases}
$$

(b) When $0 \leq c < \alpha \leq 1$ and $0 \leq r \leq (\alpha - c)/(1+\alpha)$, we have:

$$
\begin{aligned}
\widetilde{P}^s_{out} &= \frac{1-\alpha c}{1+\alpha} \\
\pi_2(d) &= \left\{ \frac{\alpha(1-\alpha c)(\alpha - c)}{(1+\alpha)^2} + (1-\alpha)\left[\frac{1}{2}\left(\frac{1+c}{1+\alpha}+d\right)^2 + \frac{1-\alpha c}{1+\alpha}\left(\frac{\alpha-c}{1+\alpha}-d\right)\right]\right\}\left(1-\frac{d}{2}\right) \\
&= -\frac{1-\alpha}{4}d^3 + \frac{(1-\alpha)(1-c)}{2}d^2 + \frac{-4c\alpha^2+2c\alpha-c^2+4c-1}{4(1+\alpha)}d + \frac{c^2-2\alpha c+1}{2(1+\alpha)} \\
\pi_2^{'}(d) &= \frac{\partial \pi_2(d)}{\partial d} = -\frac{3(1-\alpha)}{4}d^2 + (1-\alpha)(1-c)d + \frac{-4c\alpha^2+2c\alpha-c^2+4c-1}{4(1+\alpha)} \\
\Delta_2 &= [(1-\alpha)(1-c)]^2 + \frac{3(1-\alpha)(-4c\alpha^2+2c\alpha-c^2+4c-1)}{4(1+\alpha)} \\
&= \frac{(-1+\alpha)(1+2\alpha)[2\alpha(1+c+c^2)-1-4c-c^2]}{4(1+\alpha)}
\end{aligned}
$$

In area 1, we have $\Delta_2 < 0$. Thus, $\pi_2(d)$ is decreasing in d.

In area 2, 3, 4 and 5, we have $\Delta_2 > 0$. Thus, $\pi_2(d)$ is a cubic function with two extremum points $(x_3,\ x_4)$.

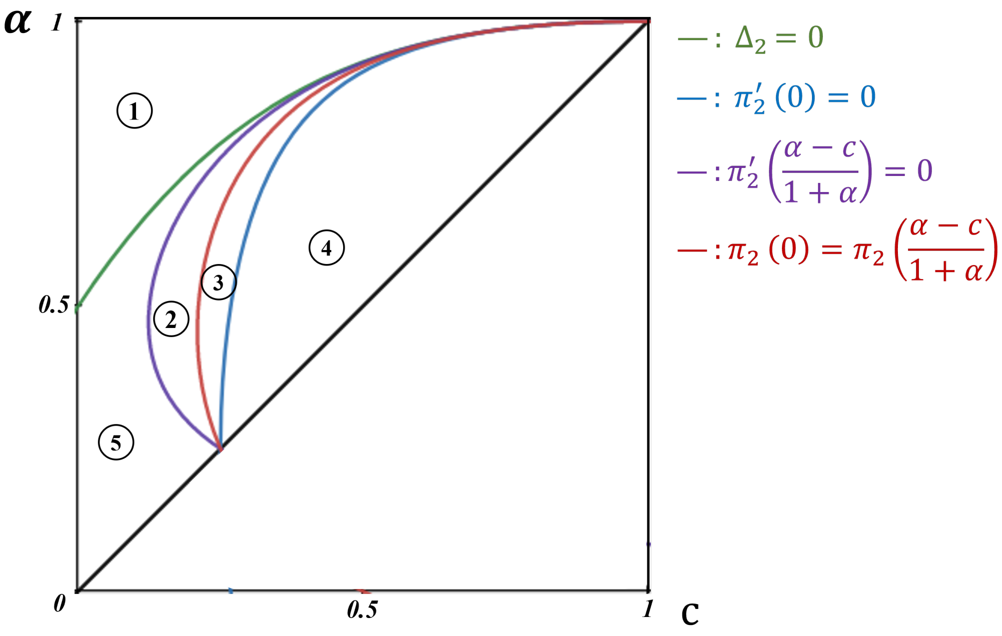
$$
\begin{aligned}
x_3 &= \frac{2[(1-\alpha)(1-c)-\sqrt{\Delta_2}]}{3(1-\alpha)} \\
x_4 &= \frac{2[(1-\alpha)(1-c)+\sqrt{\Delta_2}]}{3(1-\alpha)}
\end{aligned}
$$

Similarly, we figure out the relationship between 0, 1, x_3, x_4 and $\dfrac{\alpha-c}{1+\alpha}$ through comparing $\pi_2^{'}(0)$, $\pi_2^{'}(1)$ and $\pi_2^{'}(\dfrac{\alpha-c}{1+\alpha})$ with 0 for any $(\alpha,\ c)$ in area 2, 3, 4 and 5.

Notice that:

$$
\begin{aligned}
x_3 &< 1 \\
x_4 &> 0 \\
\frac{\alpha - c}{1+\alpha} &\leq \frac{x_3 + x_4}{2} = \frac{2(1-c)}{3} \\
\pi_2^{'}(0) &= \frac{-4c\alpha^2 + 2c\alpha - c^2 + 4c - 1}{4(1+\alpha)} \\
\pi_2^{'}(1) &= -\frac{(\alpha - c)^2}{4(1+\alpha)} < 0 \\
\pi_2^{'}(\frac{\alpha - c}{1+\alpha}) &= \frac{-a^3 - (3+4c+4c^2)\alpha^2 + (3+8c+2c^2)\alpha - 1}{4(1+\alpha)^2}
\end{aligned}
$$

Figure B.18: Case 1b and 1c ($\lambda = 0.5$)



Thus, when $0 \leq c < \alpha \leq 1$ and $0 \leq d < r \leq (\alpha - c)/(1+\alpha)$, the sub-optimal solution is:

$$
\widetilde{\pi}^s\left(\widetilde{P}^s_{out},\ \widetilde{d}^s\right) = \begin{cases} \pi\left(\dfrac{1-\alpha c}{1+\alpha},\ r - \epsilon\right), & \text{for } (\alpha,\ c) \text{ in Area 4 or 3 and } \underline{r}^2 < r \leq \dfrac{\alpha - c}{1+\alpha} \\ \pi\left(\dfrac{1-\alpha c}{1+\alpha},\ 0\right), & \text{for } (\alpha,\ c) \text{ in Areas 1, 2 and 5; or Area 3 and } 0 < r < \underline{r}^2 \end{cases}
$$

$$
\text{where } \pi\left(\frac{1-\alpha c}{1+\alpha},\ 0\right) = \pi\left(\frac{1-\alpha c}{1+\alpha},\ \underline{r}^2\right)
$$

(c) When $0 \leq c < \alpha \leq 1$ and $(\alpha - c)/(1+\alpha) < r \leq 1$, we have:

$$\pi(d) = \begin{cases} \pi_2(d), & \text{if} \quad 0 \leq d < \dfrac{\alpha - c}{1+\alpha} \\ \pi_1(d), & \text{if} \quad \dfrac{\alpha - c}{1+\alpha} \leq d < r \end{cases}$$

We need to identify the shape of $\pi_2(d)$ in $\left[0, \dfrac{\alpha - c}{1+\alpha}\right)$ and the shape of $\pi_1(d)$ in $\left[\dfrac{\alpha - c}{1+\alpha}, 1\right]$.

When $0 \leq c < \alpha \leq 1$ and $(\alpha - c)/(1+\alpha) < r \leq 1$, the sub-optimal solution is:

$$\widetilde{\pi}^s\left(\widetilde{P}^s_{out},\ \widetilde{d}^s\right) = \begin{cases} \pi\left(1 - c - min\{r, x_1\},\ min\{r, x_1\}\right), & \text{for } (\alpha,\ c) \text{ in Areas 3 and 4} \\ \pi\left(\dfrac{1-\alpha c}{1+\alpha},\ 0\right), & \text{for } (\alpha,\ c) \text{ in Areas 1 and 5} \end{cases}$$

For $(\alpha,\ c)$ in area 2, the sub-optimal solution is:

$$\widetilde{\pi}^s\left(\widetilde{P}^s_{out},\ \widetilde{d}^s\right) = \begin{cases} \pi\left(1 - c - min\{r-\epsilon, x_1\},\ min\{r-\epsilon, x_1\}\right), & \text{if } \pi_2(0) \leq \pi_1(x_1)\ and\ r > \underline{r}^1 \\ \pi\left(\dfrac{1-\alpha c}{1+\alpha},\ 0\right), & \text{otherwise} \end{cases}$$
$$where\ \pi_2(0) = \pi_1(\underline{r}^1)$$

(2) $1 - c - d < P_{out} \leq 1 - c$

The seller faces the following profit function:

$$\pi(P_{out}, d) = \left[\underbrace{\alpha P_{out}(1 - P_{out} - c)}_{\text{Profit from } S \text{ users}} + \underbrace{(1-\alpha)\int_0^1 v dv}_{\text{Profit from } NS \text{ users}}\right]\left(1 - \frac{d}{2}\right)$$

We have:

$$\widetilde{P}_{out} = max\left\{1 - c - d,\quad \frac{1-c}{2}\right\}$$

(a) when $0 \leq r \leq (1-c)/2$, $1 - c - d > (1-c)/2$; we have:

$$\widetilde{P}_{out} = 1 - c - d$$
$$\pi_1(d) = \left[\alpha(1 - c - d)d + \frac{1-\alpha}{2}\right]\left(1 - \frac{d}{2}\right)$$

According to the proof of case (1a), we need to figure out the relationship between 0, r, $\dfrac{1-c}{2}$, x_1 and x_2.

Notice that:

$$\pi_1^{'}\left(\frac{1-c}{2}\right) = \frac{-2+\alpha+2\alpha c-\alpha c^2}{8} \leq 0 \text{ for any } (\alpha,\ c) \text{ in } (0,\ 1)\times(0\ ,1).$$

$$\pi_1^{'}(0) = \frac{\partial \pi_1(d)}{\partial d}|_{d=0} = \frac{\alpha(5-4c)-1}{2}$$

$$\frac{1-c}{2} < \frac{3-c}{3} = \frac{x_1+x2}{2} < x_2$$

Thus, we have:

$$0 \leq x_1 < \frac{1-c}{2} < x_2, \quad \text{if } \alpha \geq \frac{1}{5-4c}$$

$$\text{or} \quad x_1 < 0 < r < \frac{1-c}{2} < x_2, \quad \text{otherwise}$$

Thus, when $0 \leq d < r \leq (1-c)/2$ and $1-c-d < P_{out} \leq 1-c$, we have:

$$\widetilde{\pi}^s\left(\widetilde{P}^s_{out},\ \widetilde{d}^s\right) = \begin{cases} \pi(1-c,0), & \text{if } \alpha < \dfrac{1}{5-4c} \\ \pi(1-c-min\left\{r-\epsilon,x_1\right\},min\left\{r-\epsilon,x_1\right\}), & \text{otherwise} \end{cases}$$

(b) when $r > (1-c)/2$, we have:

$$\pi(d) = \begin{cases} \left[\alpha(1-c-d)d+\dfrac{1-\alpha}{2}\right]\left(1-\dfrac{d}{2}\right), & \text{if} \quad 0 \leq d < \dfrac{1-c}{2} \\ \left[\alpha\left(\dfrac{1-c}{2}\right)^2+\dfrac{1-\alpha}{2}\right]\left(1-\dfrac{d}{2}\right), & \text{if} \quad \dfrac{1-c}{2} \leq d < r \end{cases}$$

When $\frac{1-c}{2} \leq d < r$, $\pi(d)$ is decreasing in d, therefore, in this case, the sub-optimal solution is the same as 2(a).

Thus, when $0 \leq d < r$ and $1-c-d < P_{out} \leq 1-c$, the sub-optimal solution is:

$$\widetilde{\pi}^s\left(\widetilde{P}^s_{out},\ \widetilde{d}^s\right) = \begin{cases} \pi(1-c,0), & \text{if } \alpha < \dfrac{1}{5-4c} \\ \pi(1-c-min\left\{r-\epsilon,x_1\right\},min\left\{r-\epsilon,x_1\right\}), & \text{otherwise} \end{cases}$$

(3) $1-c < P_{out}$

The seller's profit is:

$$\pi(d) = \left[(1-\alpha)\int_0^1 vdv\right](1-\frac{d}{2}) = \frac{(1-\alpha)(1-\frac{d}{2})}{2}$$

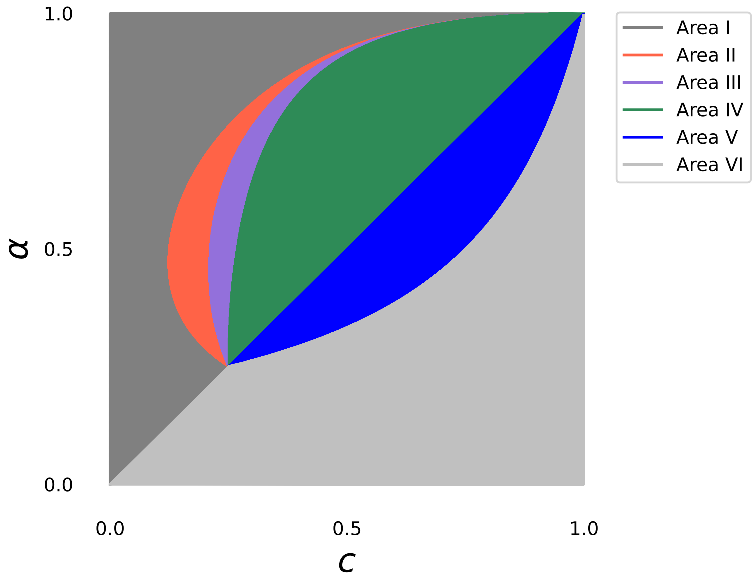
It is decreasing in d. Thus, in this case, the sub-optimal solution is:

$$\widetilde{\pi}^s\left(\widetilde{P}^s_{out},\ \widetilde{d}^s\right) = \pi(\overline{P}_{out},0)$$

$$\text{where } \overline{P}_{out} > 1-c$$

To sum up, when $0 \leq d < r$, the optimal (P_{out}, d) combination is presented in Figure B.19.

Figure B.19: Solution for $0 \leq d < r$ and $\lambda = 0.5$



For (α, c) in:

- Area I: $(\widetilde{P}^s_{out},\ \widetilde{d}^s) = \left(\dfrac{1-\alpha c}{1+\alpha},\ 0\right)$
- Area II: $(\widetilde{P}^s_{out},\ \widetilde{d}^s) = \begin{cases} \left(\dfrac{1-\alpha c}{1+\alpha},\ 0\right), \text{ if } 0 \leq r \leq max\left\{\dfrac{\alpha - c}{1+\alpha},\ \underline{r}^1\right\} \text{ or } \pi_1(x_1) \leq \pi_2(0) \\ (1 - c - min\{x_1,\ r - \epsilon\},\ min\{x_1,\ r-\epsilon\}), \text{ otherwise} \end{cases}$
- Area III: $(\widetilde{P}^s_{out},\ \widetilde{d}^s) = \begin{cases} \left(\dfrac{1-\alpha c}{1+\alpha},\ 0\right), & \text{if } 0 \leq r \leq \underline{r}^2 \\ \left(\dfrac{1-\alpha c}{1+\alpha},\ r-\epsilon\right), & \text{if } \underline{r}^2 < r \leq \dfrac{\alpha - c}{1+\alpha} \\ (1 - c - min\{x_1,\ r - \epsilon\},\ min\{x_1,\ r-\epsilon\}), & \text{if } \dfrac{\alpha - c}{1+\alpha} < r \leq 1 \end{cases}$
- Area IV: $(\widetilde{P}^s_{out},\ \widetilde{d}^s) = \begin{cases} \left(\dfrac{1-\alpha c}{1+\alpha},\ r-\epsilon\right), \text{ if } 0 \leq r \leq \dfrac{\alpha - c}{1+\alpha} \\ (1 - c - min\{x_1,\ r - \epsilon\},\ min\{x_1,\ r-\epsilon\}), \text{ otherwise} \end{cases}$
- Area V: $(\widetilde{P}^s_{out},\ \widetilde{d}^s) = (1 - c - min\{x_1,\ r - \epsilon\},\ min\{x_1,\ r-\epsilon\})$
- Area VI: $(\widetilde{P}^s_{out},\ \widetilde{d}^s) = (1 - c,\ 0)$

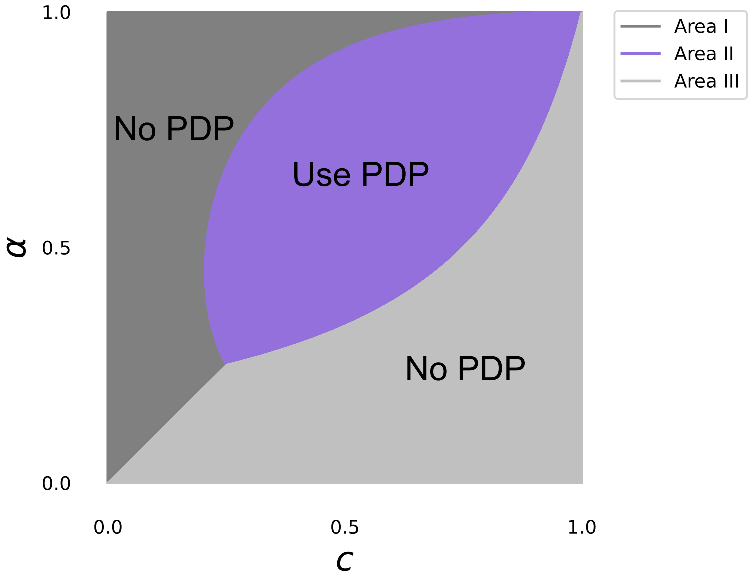
- where

  $\underline{r}^1$ is the smaller root of $\pi_2(0) = \pi_1(\underline{r}^1)$

  $\underline{r}^2$ is the smaller root of $\pi_2(0) = \pi_2(\underline{r}^2)$

We combine this sub-optimal solution from $0 \leq d < r$ and the sub-optimal solution from $d \geq r$ to figure out the global solution.

Figure B.20: Equilibrium with Sophisticated Users Under Low PDP Sensitivity ($\lambda = 0.5$)



For $(\alpha,\ c)$ in:

- Area I: $(P^{s*}_{out1},\ d^{s*}_1) = \begin{cases} (\overline{P}_{out},\ r), \text{ if } 0 \leq r \leq r_1 \\ \left(\dfrac{1-\alpha c}{1+\alpha},\ 0\right), \text{ if } r_1 < r \leq 1 \end{cases}$

- Area II: $(P^{s*}_{out2},\ d^{s*}_2) = \begin{cases} (\overline{P}_{out},\ r), \text{ if } 0 \leq r \leq r_2 \\ (1-c-x_1,\ x_1), \text{ if } r_2 < r \leq 1 \end{cases}$

- Area III: $(P^{s*}_{out3},\ d^{s*}_3) = \begin{cases} (\overline{P}_{out},\ r), \text{ if } 0 \leq r \leq 2\alpha \\ (\overline{P}_{out},\ 0), \text{ if } 2\alpha < r \leq 1 \end{cases}$

- where

  $$r_1 = \frac{2(\alpha - c^2 + 2\alpha c)}{1+\alpha}$$

$$\begin{aligned}
&r_2 = max\{x_1, 2 - 4\pi(1 - c - x_1, x_1)\}\\
&x_1 = \frac{\alpha(3 - c) - \sqrt{\Delta_1}}{3\alpha}\\
&\Delta_1 = \frac{\alpha(3\alpha + 2\alpha c^2 + 3)}{2}\\
&\overline{P}_{out} \geq 1 - c
\end{aligned}$$

B.7.2 High PDP Sensitivity ($\lambda = 2$)

When $\lambda > 1$, the feasible PDP level d is in $[0, 0.5]$.

Case 1: $d \geq r$

In this case, the sub-optimal solution is:

$$\widetilde{\pi}^s(\widetilde{P}^s_{out}, \widetilde{d}^s) = \begin{cases} \pi(\overline{P}_{out},\ r) = \dfrac{1-2r}{2}, & \text{if } 0 \leq r \leq \dfrac{1}{2} \\ 0, & \text{if } \dfrac{1}{2} < r \leq 1 \end{cases}$$
$$where\ \overline{P}_{out} \geq 1 - c$$

Case 2: $0 \leq d < r$

(1) $0 \leq P_{out} \leq 1 - c - d$

(a) When $0 \leq \alpha \leq c \leq 1$, we have:

$$\begin{aligned}
\widetilde{P}_{out} &= 1 - c - d\\
\pi_1(d) &= \left[\alpha(1 - c - d)d + (1 - \alpha)\int_0^1 vdv\right](1 - 2d)\\
&= 2\alpha d^3 - \alpha(3 - 2c)d^2 - (1 - 2\alpha + \alpha c)d + \frac{1 - \alpha}{2}\\
\frac{\partial \pi_1(d)}{\partial d} &= 6\alpha d^2 - 2\alpha(3 - 2c)d - \alpha c + 2\alpha - 1\\
\Delta_1 &= [2\alpha(3 - 2c)]^2 + 24\alpha(1 - 2\alpha + \alpha c) = 4\alpha[6 + \alpha(4c^2 - 6c - 3)] > 0\\
&\quad \text{for any } (\alpha,\ c) \text{ in } (0,\ 1) \times (0,\ 1)
\end{aligned}$$

$\pi_1(d)$ is a cubic function of d which has two extremum points $(x_1,\ x_2)$.

$$x_1 = \frac{2\alpha(3 - 2c) - \sqrt{\Delta_1}}{12\alpha}$$
$$x_2 = \frac{2\alpha(3 - 2c) + \sqrt{\Delta_1}}{12\alpha}$$

Notice that:

$$\begin{aligned} x_2 &\geq 0 \\ x_1 &< \frac{1}{2} \\ \pi_1^{'}(0) &= -1 - \alpha(c-2) \leq 0 \text{ for } 0 \leq \alpha \leq c \leq 1 \\ \pi_1^{'}\left(\frac{1}{2}\right) &= \frac{\alpha(1+2c)-2}{2} \\ \pi_1(0) > \pi_1\left(\frac{1}{2}\right) &= 0 \end{aligned}$$

Thus, when $0 \leq \alpha \leq c \leq 1$ and $0 \leq d < r$, the sub-optimal solution is:

$$\widetilde{\pi}^s(\widetilde{P}^s_{out},\ \widetilde{d}^s) = \pi(1-c, 0)$$

(b) When $0 \leq c < \alpha \leq 1$ and $0 \leq r \leq (\alpha - c)/(1+\alpha) \leq 0.5$, we have:

$$\begin{aligned} \widetilde{P}^s_{out} &= \frac{1-\alpha c}{1+\alpha} \\ \pi_2(d) &= \left\{\frac{\alpha(1-\alpha c)(\alpha - c)}{(1+\alpha)^2} + (1-\alpha)\left[\frac{1}{2}\left(\frac{1+c}{1+\alpha}+d\right)^2 + \frac{1-\alpha c}{1+\alpha}\left(\frac{\alpha-c}{1+\alpha}-d\right)\right]\right\}(1-2d) \\ &= -(1-\alpha)d^3 + \frac{(1-\alpha)(1-4c)}{2}d^2 - \frac{(1-c)^2+(1-\alpha)^2c}{1+\alpha}d + \frac{c^2-2\alpha c+1}{2(1+\alpha)} \\ \pi_2^{'}(d) &= -3(1-\alpha)d^2 + (1-\alpha)(1-4c)d - \frac{(1-c)^2+(1-\alpha)^2c}{1+\alpha} \\ \Delta_2 &= \frac{(-1+\alpha)[(1+4c+16c^2)\alpha^2 - 24c\alpha - 4c^2 - 4c + 11]}{1+\alpha} \end{aligned}$$

Notice that, when $\Delta_2 > 0$:

$$\begin{aligned} x_3 &= \frac{(1-\alpha)(1-4c) - \sqrt{\Delta_2}}{6(1-\alpha)} < 0 \\ \pi_2^{'}(0) &= -\frac{(1-c)^2+(1-\alpha)^2c}{1+\alpha} < 0 \\ \pi_2^{'}\left(\frac{1}{2}\right) &= \frac{(1+4c)\alpha^2 + 8c\alpha - 4c^2 - 4c - 5}{1+\alpha} < 0 \\ \pi_2^{'}(\frac{\alpha-c}{1+\alpha}) &= \frac{(2+3c)a^3 - (3+4c+4c^2)\alpha^2 + (5+2c)c\alpha - 1}{(1+\alpha)^2} < 0 \end{aligned}$$

Therefore, $\pi_2(d)$ is decreasing in d when $0 \leq c < \alpha \leq 1$ and $0 \leq d < r \leq (\alpha - c)/(1+\alpha)$, the sub-optimal solution is:

$$\widetilde{\pi}^s\left(\widetilde{P}^s_{out},\ \widetilde{d}^s\right) = \pi\left(\frac{1-\alpha c}{1+\alpha},\ 0\right)$$

(c) When $0 \leq c < \alpha \leq 1$ and $(\alpha - c)/(1+\alpha) < r \leq 1$, we have:

$$\pi(d) = \begin{cases} \pi_2(d), & \text{if } \quad 0 \leq d < \dfrac{\alpha - c}{1+\alpha} \\ \pi_1(d), & \text{if } \quad \dfrac{\alpha - c}{1+\alpha} \leq d < r \leq \dfrac{1}{2} \\ 0, \text{ if} \dfrac{1}{2} < d \end{cases}$$

According to the proof of case (1b), $\pi_2(d)$ is decreasing in $\left[0, \dfrac{\alpha - c}{1+\alpha}\right)$.
When $0 \leq c < \alpha \leq 1$ and $(\alpha - c)/(1+\alpha) < r \leq 1$, the sub-optimal solution is:

$$\widetilde{\pi}^s\left(\widetilde{P}^s_{out},\ \widetilde{d}^s\right) = \pi\left(\frac{1 - \alpha c}{1+\alpha},\ 0\right)$$

(2) $1 - c - d < P_{out} \leq 1 - c$

$$\pi(P_{out}, d) = \left[\underbrace{\alpha P_{out}(1 - P_{out} - c)}_{\text{Profit from } S \text{ users}} + \underbrace{(1-\alpha)\int_0^1 v dv}_{\text{Profit from } NS \text{ users}}\right](1 - 2d)$$

$$\widetilde{P}_{out} = max\left\{1 - c - d,\ \frac{1-c}{2}\right\} = \frac{1-c}{2}$$

$\pi(d)$ is decreasing in d when $d \in [0, 0.5]$. Thus, when $0 \leq d < r$ and $1 - c - d < P_{out} \leq 1 - c$, the sub-optimal solution is:

$$\widetilde{\pi}^s\left(\widetilde{P}^s_{out},\ \widetilde{d}^s\right) = \pi(1 - c, 0)$$

(3) $1 - c < P_{out}$
The seller's profit is:

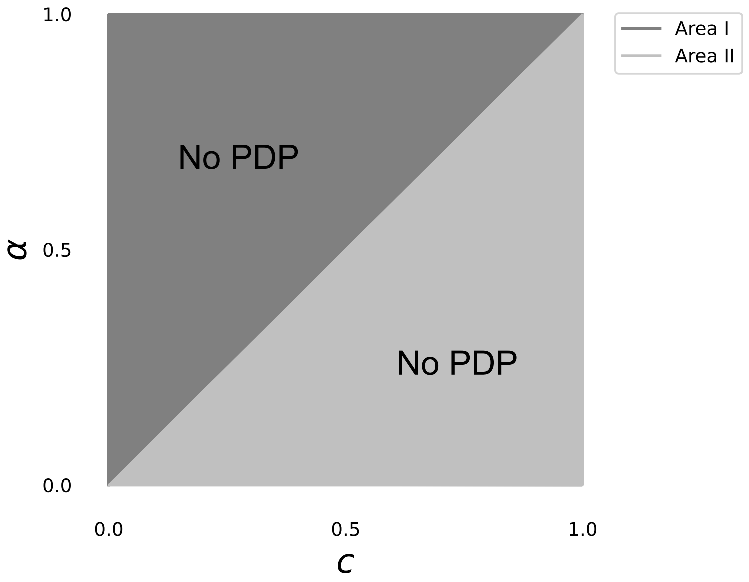
$$\pi(d) = \left[(1-\alpha)\int_0^1 v dv\right](1 - 2d) = \frac{(1-\alpha)(1-2d)}{2}$$

It is decreasing in d. Thus, in this case, the sub-optimal solution is:

$$\widetilde{\pi}^s\left(\widetilde{P}^s_{out},\ \widetilde{d}^s\right) = \pi(\overline{P}_{out}, 0)$$
$$\text{where } \overline{P}_{out} > 1 - c$$

We combine this sub-optimal solution from $0 \leq d < r$ and the sub-optimal solution from $d \geq r$ to figure out the global solution.

Figure B.21: Equilibrium with Sophisticated Users Under High PDP Sensitivity ($\lambda = 2$)



For $(\alpha,\ c)$ in:

- Area I: $(P^{s*}_{out1},\ d^{s*}_1) = \begin{cases} (\overline{P}_{out},\ r),\ \text{if } 0 \le r \le r_1 \\ \left(\dfrac{1-\alpha c}{1+\alpha},\ 0\right),\ \text{if } r_1 < r \le 1 \end{cases}$
- Area II: $(P^{s*}_{out2},\ d^{s*}_2) = \begin{cases} (\overline{P}_{out},\ r),\ \text{if } 0 \le r \le \dfrac{\alpha}{2} \\ (\overline{P}_{out},\ 0),\ \text{if } \dfrac{\alpha}{2} < r \le 1 \end{cases}$
- where

  $r_1 = \dfrac{\alpha - c^2 + 2\alpha c}{2(1+\alpha)}$

  $\overline{P}_{out} \ge 1 - c$