systems

MDPI

Article

Evolutionary Analysis of the Regulation of Data Abuse in Digital Platforms

Zhen Wang [1], Chunhui Yuan [1,*] and Xiaolong Li [2]

[1] School of Economics and Management, Beijing University of Posts and Telecommunications, Beijing 100087, China; wangzhen09@bupt.edu.cn
[2] School of Modern Post, Beijing University of Posts and Telecommunications, Beijing 100087, China; xiaolongli@bupt.edu.cn
* Correspondence: yuanchunhui@bupt.edu.cn

Abstract: This study proposes a tripartite evolutionary game model to investigate the interactions among digital platforms, governments, and users to address the negative consequences of data abuse. The paper identifies that the high tax incentives and low penalties set by the government will increase the incentive for data abuse by platforms of different sizes, and the government can try to set up a tax ladder policy for platforms of different sizes and a dynamic penalty amount based on platform revenue. The study also reveals that user participation in supervision can reduce information asymmetry, and decrease the cost of government regulation. However, the single constraint of users is less effective than government regulation or dual user-government regulation. Additionally, the presence of privacy leakage risks prompts digital platforms to adopt compound engines to implement data abuse. Hence, the relevant government regulatory policies should consider the efficiency and cost of data security technology for timely adjustments. This research contributes to understanding the complex relationships among digital platforms, governments, and users and highlights the need for appropriate measures to mitigate the negative effects of data abuse.

Keywords: data abuse; digital platforms; risk of privacy leakage; governance mechanisms

Citation: Wang, Z.; Yuan, C.; Li, X. Evolutionary Analysis of the Regulation of Data Abuse in Digital Platforms. *Systems* **2023**, *11*, 188. https://doi.org/10.3390/systems11040188

Academic Editors: Shaojian Qu, Ying Ji and M. Faisal Nadeem

Received: 10 March 2023
Revised: 3 April 2023
Accepted: 3 April 2023
Published: 7 April 2023

1. Introduction

In recent years, the increasing prevalence of data scandals on digital platforms has brought data abuse and privacy security to the forefront of public attention. Unlike traditional economic models, digital platforms are characterized by the collection, processing, and mining of data through complex algorithms, which results in economic value. The more data a platform collects, the greater the economic value it can obtain, which enhances its market power [1]. The availability of data resources significantly influences the formation of competitive economic structures for platforms. Consequently, data competition [2], non-monetary transactions [3], and privacy protection have become crucial issues that affect the market dominance of platforms [4–6]. In this context, some platforms may choose to abuse data to achieve monopolistic profits. This phenomenon has become increasingly common and has resulted in several high-profile cases. For instance, in July 2022, the State Internet Information Office of China imposed a fine of RMB 8.026 billion on Didi Global Inc., which was found to have engaged in 16 illegal activities across eight categories. Specifically, Didi Global Inc. collected users' face recognition information, precise location information, and affinity information through illicit means, seriously violating users' personal information rights and interests. This action underscores the importance of data security for digital enterprises and brings public concerns about data abuse on digital platforms to the forefront.

Data abuse refers to the unauthorized acquisition and use of personal data by enterprises, organizations, or individuals, including but not limited to identity information, transaction records, and health records, without the explicit consent of users. From the

perspective of competition law, data abuse can be classified into two categories: exploitative abuse and exclusive abuse [7]. Exploitative abuse occurs when digital platforms exploit their platforms to extract consumer benefits in the process of users exchanging data for the right to use digital services. In practice, consumers have limited choices when it comes to data sharing and are forced to accept the data equivalents unilaterally set by the platform. This can lead to excessive collection of personal information and even data-related harm. On the other hand, exclusionary abuse focuses on the tactics used by digital platforms to restrict competition by leveraging their data advantage, such as exclusive contracts, cross-use of data, and refusal to share data. Table 1 outlines the common practices and main hazards of exploitative and exclusive abuses.

Table 1. The common practices and main hazards of data abuse

Type	Practice	Main Hazards	Example Case
Exploitative Abuse	Big Data Price Discrimination	Violation of consumers' fair trading rights	The case of Trip.com Group (2021)
	Advertising Abuse	Reducing the user's experience and comfort	Excessive advertising in Wechat Moments (2018)
	Surveillance Abuse	Personal privacy rights are violated	NSO Group's Pegasus (2021)
Exclusive Abuse	Exclusive Contract	Restricting consumer choice and undermining fairness	"Two choose one" of Meituan (2021)
	Cross-Use of Data	Aggravating the coordinated monopoly of top platforms	Google and Facebook's duopoly (2019)
	Refusal to Share Data	Violating the "essential facilities" principle	HiQ Labs, Inc. v. LinkedIn Corp. (2019)

Table 1 illustrates how data abuse by digital platforms has negatively impacted both consumer rights protection and platform economic development. Exploitative abuses, such as the case of Trip.com, excessive collection of personal information by the Wechat Moments, and the Pegasus software spying scandal, violate consumers' right to fair trade and personal privacy. Given the prevalence of personal information, including home addresses, vehicle information, telecommunication information, and courier information, it is evident that consumers face substantial risks of having their personal data used for commercial purposes without their consent. However, relevant companies have yet to provide adequate protection against illegal data extraction and sale. This poses a serious impediment to the growth of the platform economy, as consumers increasingly seek to limit their online footprint to mitigate data abuse concerns [8]. In addition, the existence of exclusionary abuses, exemplified by cases such as the 'Two choose One' case and the Google and Facebook synergistic monopolies, exacerbates data monopolies, inhibits industry innovation, squeezes the viability of SMEs, jeopardizes fair competition in the marketplace, and disrupts market order. As a result, governing the data abuse behaviors of digital platforms has become a critical issue for the development of the platform economy.

Why does data abuse happen? Scholars have undertaken extensive research into the causes of data abuse and have identified three main factors. Firstly, the profit-seeking nature of platforms. Since the platform has the characteristics of strong network externality [9], multi-attribution of users [10], winner-take-all [11], etc., the valorization of the data can enhance its market power, so the digital platform has the motive to commit data abuse in pursuit of monopoly profits. Secondly, the government values efficiency over equity. Usually, the government provides a variety of preferential policies and a relaxed regulatory environment for platforms to improve their market efficiency. For example, the Chinese government offers a preferential tax rate of 10% for some platforms [12], which leaves the door open for platforms to abuse data. Thirdly, users relinquish ownership of their data. Users enjoy services without being concerned about privacy exposure. On the one hand, the data collected by the platform improves the user services. On the other hand,

this data is accessed by third parties in a way that harms users and generates the risk of user privacy leakage [13,14]. The trade-off between good service and loss of privacy is a game-theoretic choice of whether users choose to participate in the supervision of data abuse on platforms. Overall, the abuse of data on digital platforms occurs as a result of a game of multiple forces.

Moreover, the previous studies has conducted extensive research on the regulation of data abuse from various perspectives. For instance, Inge Graef [7] suggested that revamping competition law may be an appropriate mechanism to address data abuse from a legal framework perspective. However, competition law, which takes an economic approach based on effects and mainly considers economic efficiency factors, may not take into account the interests of other stakeholders in the data abuse process. In actual regulatory practice, other regulatory mechanisms, such as data protection and consumer protection regulations, must be used and enforced concurrently. From a technological innovation and standardization research perspective, some scholars, such as Wang et al. [15], have proposed technical interventions to stop data abuse, including a smart contract token-based solution to achieve secure dynamic access control for industrial IoT systems. Nonetheless, technological solutions serve only as auxiliary means of regulation and cannot eliminate the occurrence of data abuse entirely. In practice, government regulatory mechanisms should still be the dominant approach. For example, Liu et al. [16] studied the issue of big data fraud and proposed regulating tax rates and penalties. Increasing the tax rate would inhibit the expansion of enterprise scale and weaken the motivation of platforms to misuse data. However, this approach did not consider the privacy risks involved. Overall, while scholars have made progress in the study of data abuse and its regulation on digital platforms, existing literature has yet to consider the power dynamics among the government, users, and platforms. Additionally, little attention has been paid to the relationship between the role of factors such as the tax rate preferences granted by the government to platforms and the loss of privacy leakage suffered by users and platforms in both directions in the tripartite decision.

In fact, digital platforms are based on data and algorithms to provide services to users [17–19], and users play a pivotal role in platform regulation due to their unique advantage in accessing platform information, which can effectively reduce information asymmetry [20]. Users' participation in platform regulation is a valuable complement to government regulation, especially in cases of capacity or resource deficiencies. Nevertheless, limited enforcement power for independent and effective regulations poses a challenge. Therefore, breaking capacity bottlenecks and traditional regulatory fragmentation and implementing collaborative regulation between government and users represent a new regulatory paradigm. Essentially speaking, the governance problem of data abuse in digital platforms can be conceptualized as a tripartite evolutionary game model, which is dynamic and evolves over time. The assumptions of bounded rationality and the dynamic evolution of evolutionary game theory align well with the behavior and decision-making characteristics of all parties involved in data abuse. Therefore, evolutionary games provide an excellent representation of reality and a robust framework that can well represent the reality and further explore the regulatory mechanism of data abuse on digital platforms. Based on this, this study conceptualizes the data abuse of digital platforms as a dynamic process and constructs a tripartite evolutionary game model to examine the regulatory mechanisms. The study aims to address the following questions: (1) What are the significant factors that influence a digital platform's decision to abuse data, such as the platform's profits and the government's tax rate? (2) How can we design effective regulatory mechanisms to stop platforms from committing data abuse?

The rest of this paper is organized as follows. Section 2 provides a comprehensive review of the relevant research in this field. In Section 3, the issue is carefully examined and an evolutionary game model is constructed accordingly. The analytical results for the evolutionarily stable strategiesESSs in the evolutionary game are presented in Section 4.

Section 5 provides a numerical simulation, and conclusions and managerial implications are given in Section 6.

2. Literature Review

With the booming platform economy, the governance of digital platforms has become a top priority for policymakers, regulators, and competition authorities around the world. The vast literature on digital platform governance explores issues such as merger and acquisition, pricing [5,20], collusion [21], and the abuse of market dominance [22]. This study focuses on the governance of data abuse in digital platforms, referring to the harmful effects that can arise from the excessive collection or use of user data. In the platform economy, it is manifested as excessive collection of user data [23,24], refusal to share data, use of data advantages to achieve self-preferential treatment, forced free-riding, big data discrimination pricing [16], the abuse of market leverage, etc. Instead of analyzing the specific harm of each form of data abuse, this paper employs evolutionary game theory to explore key factors that influence the decision making of governments, platforms, and users in different data use scenarios. Additionally, it examines the mechanisms that governments and users can employ to prohibit platforms from data abuse. The relevant literature includes three aspects: research on the motivation for data abuse by platforms, research on the regulation of data abuse by platforms, and research on evolutionary game model.

2.1. Research on the Motivation for Data Abuse by Platforms

The research on the motivation behind why digital platforms choose to abuse data is fragmented, as scholars often focus on single factors or subjects. There is currently no systematic research framework in place. Therefore, this paper aims to combine relevant literature to identify the relevant motives that scholars have discussed. These motives can be broadly categorized into two groups: direct factors and indirect factors. One of the direct factors is data-based revenue, as data is considered an indispensable factor of production in the platform economy [25]. It directly contributes to economic growth and enhances the efficiency of social production in enterprises [1]. So, the digital platform has the appeal of data valorization. However, enterprises are inherently profit-seeking, and in order to capture more value, a few platforms that have strong market power choose to abuse data to maximize their revenue [22]. On the other hand, indirect factors, such as government policy and user behavior, also influence the data use strategies of platforms. Government policies, such as tax rates and penalties, can indirectly influence their data use strategies by affecting the platform's profits. [16,26] argued that charging different tax rates on access revenue and data use revenue will reduce platforms' incentives to over-collect personal data. Liu, W. et al. [16] considered that high fines reduce the profitability of the platform by reducing the revenue from a breach and thereby stopping the platform companies from carrying out data abuse. Similarly, the user's privacy exposure [8] affects the platform's ultimate data usage strategy by influencing the amount of data available to the platform. Bourreau, M. et al. [27] believed that the data provided to the platform by users during their consumption on the platform is used to optimize business and increase market power. Once users reduce consumption or falsify consumption data, this will reduce the revenue that the platform obtains from the data, and thus, reduce the incentive for the platform to carry out data abuse.

2.2. Research on the Regulation of Data Abuse by Platforms

There are many regulatory studies on data abuse on digital platforms, and a variety of regulatory paths been have proposed. They can be mainly divided into two categories: platform technical interventions and government policy interventions.

On the technical front, scholars have proposed a range of measures to regulate data abuse. Some examples include differential privacy protection technology [28], which effectively safeguards user privacy on digital platforms; blockchain encryption technology [29–31], which encrypts and protects data from malicious access and exploitation; and,

machine learning algorithms-based attacker detection methods [32], which identify issues in data collection, storage, processing, and sharing. On the government front, policymakers can adopt several measures to curb data abuse. For instance, Liu, W. et al. [16] proposed to regulate tax rates, which would discourage firms from expanding and thus weaken the incentive for platforms to abuse data. However, the tax system in many countries is still highly controversial. This path may not be a feasible solution. Another proposed approach, suggested by Grewal, R. et al. [33], is to regulate the amount of fines and urged the government to exercise the administrative punishment functions, but the standard of fines is still inconclusive, as evidenced by the current penalty strategy in China, which follows a "one case one meeting" approach. Shi, T. et al. [34] believed that data privacy policies can be adjusted and that strict privacy protection policies will increase the cost of violations for data abuse of digital platforms, but discourage innovation. Obviously, there are multiple trade-offs in the process of platform economic development [35]. The above research affirms the leading role of the government in supervision, but does not take into account the conflicting interests between the government, the platform and users. There is a certain power game among the three parties, and the design of the supervision mechanism also needs to focus on the game relationship between the three. Overall, a more comprehensive and nuanced approach is needed to effectively regulate data abuse on digital platforms, which takes into account the interests of all parties involved and considers the potential unintended consequences of various regulatory paths.

2.3. Research on Evolutionary Game Theory

Evolutionary game theory is a tool utilized in the study of interactions between animals, humans, and other organisms with regards to their behavioral strategies [36]. Common forms are bipartite evolutionary game models [37,38], tripartite evolutionary game models [39,40], etc. In such games, the choices made by one organism can notably affect the actions of others, ultimately leading to varying levels of success or failure in terms of individual survival and reproductive outcomes within a population. Therefore, the evolutionary game method [37,39,40], which focuses on the evolutionary process and stable state of the population, can help to study the cooperation [41], competition [42,43] and regulation [44–46] in social and commercial decision making. Concerned that the problem of data abuse involves a game between the government, platforms and users, which form a limited and large group, the evolutionary game approach can be used to explore the regulatory mechanism to stop data abuse on digital platforms.

In summary, scholars have made some achievements in research on data abuse and its regulation of digital platforms. However, the existing literature contains more research from unilateral or two parties while less consideration is given to the three-party power game between the government, users, and the platform. Meanwhile, no attention is paid to the relationship between the role of factors such as the tax benefits given by the government to the platforms and the loss of privacy leakage suffered by users and platforms in the decision-making of the three parties; therefore, the current available research lacks a systematic and dynamic research approach.

3. Methodology

This study focus on the design of supervision mechanisms for preventing digital platforms from abusing data, and considers the data-based role relationship between platforms, governments, and users.

3.1. Evolutionary Game

Evolutionary game is a game model that describes the long-term adaptation and evolution of game participants. Based on the interaction and selection among game participants, the model simulates the long-term evolution among them through a series of evolutionary rules and strategies. Evolutionary game theory assumes that there is a group of n independent individuals $d = \{d_1, d_2, \ldots, d_n\}$ playing against each other.

All players use pure strategies, and the set of pure strategies that players can choose is $S = \{s|s = 1, 2, \ldots, k\}$. At some point t, the proportion of individuals in the group choosing various strategies is $X = \{x_1, x_2, \ldots, x_k\}$. The set of individuals who choose a particular strategy is called as an aggregate, and $U = (s = k)$ denotes the overall return when strategy k is chosen, then the average return of the whole group is expressed as Equation (1),

$$\overline{U} = \sum_{i=1}^{k} x_i \times U(s = i). \tag{1}$$

According to evolution theory, the population size of a group will change over time t, and the proportion of individuals choosing each strategy x will also change accordingly. The rate of change in the number of individuals in the population is called the replicator dynamics ($F(x_k)$), which can be calculated as Equation (2). The variable k_x represents the probability that an individual initially adopts strategy k. $U(i = k)$ denotes the expected payoff for an individual who chooses strategy k, which is the average value. The stable state of population evolution is represented by the replication dynamic equation equaling zero; that is, the replication rate is zero. Different stable states of the equation have varying degrees of robustness. A stable point in the convergence state is referred to as an Evolutionary Stable Strategy (ESS) [42,47].

$$F(x_k) = \frac{dx_k}{dt} = x_k[U(i = k) - \overline{U}(i = k)]. \tag{2}$$

Evolutionary game theory is based on the principles of neighborhood interaction and adaptability, where the behavior of an individual or group is influenced by others in their surroundings and they adapt their strategy choices accordingly. This theory is highly suitable for studying conflicts that arise in the process of data use among digital platforms, governments, and users, as their actions are mutually influenced and dynamically evolved. The model provides a mathematical framework to analyze the behavior of this complex system, especially in revealing the long-term decision-making mechanisms of limited rationality stakeholders in the dynamic game process of data abuse.

3.2. Basic Assumptions

Digital platforms serve as intermediaries between users and sellers, where users provide data to the platform while utilizing its services, such as purchasing, commenting, or clicking on ads. This data is used by platforms to improve services, personalize recommendations and provide targeted advertising. Governments play a critical role in regulating digital platforms, ensuring fair competition, protecting user privacy, and enforcing legal standards for data collection and usage. They tax platforms and investigate or penalize those that violate the legal standards. As ultimate data providers, users have the right to choose the platforms they use, the data they provide, and the products or services they purchase. However, users face risks such as data breaches, identity theft, and exposure to harmful content. Therefore, they rely on platforms and governments to protect their interests and assert their rights. The logical relationships between the players are shown in Figure 1. The dynamic and complex relationship between platforms, governments, and users requires analysis through a suitable mathematical model that captures the interactions between participants seeking to maximize their interests while minimizing costs and risks.

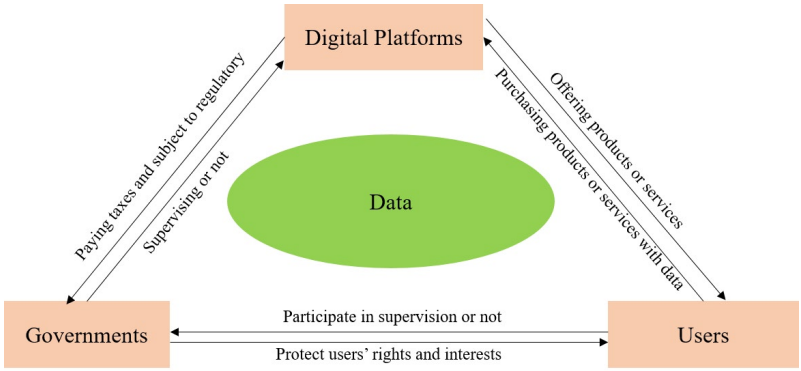


Figure 1. The logical relationship between the players of the tripartite evolutionary game.

The study explores the issue of data abuse in the virtual realm of the network, which implicates the interests of three parties: the platform, the government, and users. In view of the distinctive objectives and perspectives of these three stakeholders, there is a natural tendency for each party to engage in adaptive learning behavior. Specifically, in the real-world scenarios, the platforms exhibit a profit-oriented mindset and may potentially resort to data abuse as a means to maximize their earnings. On the other hand, the government needs to invest significant human and material resources to monitor and control the use of data, and their ultimate goal is to promote regulatory efficiency, which comes at a cost. Users, in turn, may not perceive the negative consequences of privacy violations but instead prioritize the quality of services and the personal benefits derived from the use of platforms. Given the differences in the objectives of the three parties and the resulting information asymmetry among them, we formulate the following hypotheses based on our analysis.

Hypothesis 1. The players of the game and their strategies. The players of the game are the governments, the digital platforms, and the users, all of which employ bounded rationality. With reference to the setup of Liu et al. [16], the parties' decisions are independent and made under asymmetric information; that is, in the current game process, the players cannot grasp the strategic information of the other player and are affected by the results of the previous game. The government's space of choices of strategy, with corresponding probabilities, is S_1 = {Supervise x, Not supervise $1-x$}. The decision space of the platform's strategies, with the corresponding probabilities, is S_2 = {Abuse data y, Not abuse data $1-y$}. The user's strategy space, with the corresponding probabilities, is S_3 = {Participate in supervision z, Not participate in supervision $1-z$}. Moreover, we assume that $x, y, z \in [0,1]$.

Hypothesis 2. Benefit and cost structure of the government. The government's supervisory actions incur costs C_g, such as the cost of information in the process of collecting evidence and the cost of human and material resources in the process of enforcement. Simultaneously, regulation can also bring the government an income F from fines, and certain social benefits K, such as an increase in the government's credibility, the maintenance of market order, etc. However, it should be noted that the government has an incentive to regulate only when the benefits of regulation are greater than the costs. And when the government does not supervise the data abuse of the platforms, resulting in there being no way to appeal for users who actively participate in supervision, the government will have a certain loss of reputation C_n, which is manifested as a poor relationship between the government and the public and a worsening of the government's image, etc.

Hypothesis 3. Benefit and cost structure of digital platforms. The motivation for digital platforms to abuse data is to gain more revenue R_2, which can help it expand its data advantage and improve its operational efficiency and market position [48]. At the same time, the platform also needs to pay additional technical processing costs C_p and bear some risk of privacy breach L_p. It is known from practice that the revenue R_2 obtained by digital platforms when they abuse data to carry out business activities is greater than the revenue R_1 obtained by their compliant use of data, and at the time when the government

intervenes to regulate them, they need to pay a fine F and pay a compensation s demanded by users. In addition, according to van Hoboken & Fathaigh [24], there is the risk of privacy leakage in the process of data collection and application by digital platforms. The risk of privacy leakage when the platform chooses to abuse data α is greater than the risk when the enterprise does not abuse data β, and if privacy leakage occurs, it will cause bilateral loss to the enterprise and the user.

Hypothesis 4. Benefit and cost structure of users. When the platform carries out data abuse, the user's utility is compromised, changing from U_2 to U_1. Referring to Cloarec [13], we consider that in the context of supervision, users need to pay the information cost C_u for collecting relevant evidence, while gaining supervision benefits A, such as moral satisfaction and reputation enhancement, etc. Some government-oriented user monitoring behavior (such as reporting, complaints, etc.) will gain government incentives H once data abuse of digital platforms is effectively reported; platform-oriented monitoring behavior (such as bad reviews, refusal to provide data, providing false data, etc.) is made possible by refusing to provide a portion of the data e to the platform, resulting in the platform suffering some loss of revenue based on the data. If users do not participate in supervision, the platform will have no data-based revenue loss.

Hypothesis 5. The characteristics of the decision makers. The decision makers of the government, platforms and users in the model are risk-neutral and constitute a limited but large population, and their goals are to maximize their own benefits. In addition, the decision makers are incompletely rational, and no cooperative relationship between the parties is fixed for a long time. There is a learning mechanism in the whole process of the game, and the players can adjust their strategies according to their past experience in the game to obtain the maximum degree of adaptation in the game.

The symbols used in the model are shown in Table 2.

Table 2. Parameters of the tripartite evolutionary game between a government, digital platforms and users.

Symbol	Notation
x	Probability of supervision by government
y	Probability of platforms abuse data
z	Probability of users participate in supervision
R_1	Revenue when platforms abuse data
R_2	Revenue when platforms do not abuse data
s	Percentage of users claiming compensation when platforms abuse data
r	Tax rate of the platform
C_p	Cost of technology when platforms abuse data
α	Risk of privacy breaches when platforms abuse data
β	Risk of privacy breaches when platforms do not abuse data
L_p	Loss of platform in case of privacy breach
U_1	Utility of users when platforms abuse data
U_2	Utility of users when platforms do not abuse data
C_u	Information costs when users participate in supervision
e	Probability of users refusing to provide data
H	Rewards to the government when users participate in supervision
A	Benefits of self-efficacy for users participate in supervision
C_g	Cost of the government's supervision
F	Penalty for platforms abusing data
K	Social benefits of government's supervision
C_n	Loss of reputation of government when users participate in supervision
L_u	Loss of users in case of privacy breach

3.3. Payoff Matrix

Based on the above assumptions and parameter settings, the payoff matrix for each player when the platform abuses data is shown in Table 3, whereas Table 4 depicts the situation when the platform refrains from such behavior.

Table 3. Payoff matrix for both players when digital platforms abuse data.

		Governments	
		Supervise x	**Not Supervise $1-x$**
Users	PS (z)	$(1-e)rR_1 - C_g + F + K - H$ $(1-r)R_1 - C_p - F - \alpha L_p$ $U_1 + -\alpha L_u$	$(1-e)rR_1 - C_n$ $(1-e)(1-r)R_1 - C_P - \alpha L_p$ $U_1 + A - C_u - \alpha L_u$
	NPS ($1-z$)	$rR_1 - C_g + F + K$ $(1-r)R_1 - C_p - F - \alpha L_p$ $U_1 - \alpha L_u$	rR_1 $(1-r)R_1 - C_p - \alpha L_p$ $U_1 - \alpha L_u$

Note: The PS refers to "Participate in supervision". The NPS refers to "Not participate in supervision".

Table 4. Payoff matrix for both players when digital platforms don't abuse data.

		Governments	
		Supervise x	**Not Supervise $1-x$**
Users	PS (z)	$(1-e)rR_2 - C_g + K - H$ $(1-e)(1-r)R_2 - \beta L_p$ $U_2 + A - C_u - \beta L_u + H$	$(1-e)rR_2$ $(1-e)(1-r)R_2 - \beta L_p$ $U_2 + A - C_u - \beta L_u$
	NPS ($1-z$)	$rR_2 - C_g + K$ $(1-r)R_2 - \beta L_p$ $U_2 - \beta L_u$	rR_2 $(1-r)R_2 - \beta L_p$ $U_2 - \beta L_u$

Note: The PS refers to "Participate in supervision". The NPS refers to "Not participate in supervision".

4. Analysis of the Evolutionary Stability Strategy

4.1. Evolutionary Stability Strategies of the Government

According to assumptions 1–5 and Tables 3 and 4, the expected return E_x for the government from choosing the "Supervise" strategy, the expected return E_{1-x} for the "Not supervise" strategy, and the average expected return E_g in the game are:

$$E_{1-x} = yz[(1-e)rR_1 - C_n] + y(1-z)rR_1 + (1-y)z(1-e)rR_2 + (1-y)(1-z)rR_2, \quad (3)$$

$$\begin{aligned} E_x = {} & yz[(1-e)rR_1 - C_g + F + K - H] + y(1-z)[(1-e)rR_1 - C_g + F + K] \\ & + (1-y)z[(1-e)rR_2 - C_g + K - H] + (1-y)(1-z)(rR_2 - C_g + K), \end{aligned} \quad (4)$$

$$E_g = xE_x + (1-x)E_{1-x}. \quad (5)$$

The equations for the replication dynamics of the government are obtained according to the Malthusian equation as follows:

$$F(x) = x(E_x - E_g) = x(1-x)(K - C_g + yF + yzC_n - yzH), \quad (6)$$

differentiating with respect to x yields

$$\frac{d(F(x))}{dx} = (1-2x)(K - C_g + yF + yzC_n - yzH). \quad (7)$$

Based on the stability theorem, x is an Evolutionarily Stable Strategy (ESS) when $F(x) = 0$ and $\frac{d(F(x))}{dx} \leq 0$. Letting $F(x) = 0$, we get $x = 0$, $x = 1$ or $y = \frac{C_g - K}{F + z(C_n - H)} = y^*$, and we can see that when $y = y^*$, for any x we have $F(x) = 0$ and $\frac{d(F(x))}{dx} = 0$. Any strategy of the government is a stable strategy. When $y < y^*$, $\frac{d(F(x))}{dx}|_{x=0} < 0$, $\frac{d(F(x))}{dx}|_{x=1} > 0$, and so $x = 0$ is the ESS of the government. Conversely, when $y > y^*$, $x = 1$ is the ESS.

Based on the above analysis, a phase diagram can be constructed to depict the dynamic change process of the government's strategy, as shown in Figure 2. In the figure, $y = \frac{C_g - K}{F + z(C_n - H)} = y^*$ forms a surface on which any strategy chosen by the government is stable, while we can see that the surface divides the cubic space into two regions V_1 and V_2. In region V_1, the government's strategy will be stable in the "Supervise" strategy, while in region V_2, the government's strategy is stable in the "Not supervise" strategy.

Analysis shows that government regulatory strategy is effective based on fines F and user participation z, but negatively affected by regulatory costs C_g and user incentives H. Current fines for platform enterprises are ineffective due to their high market value. Regulations should be revised to align fines with turnover and revenue, and innovative technology and user incentives should be used to reduce costs and increase participation.

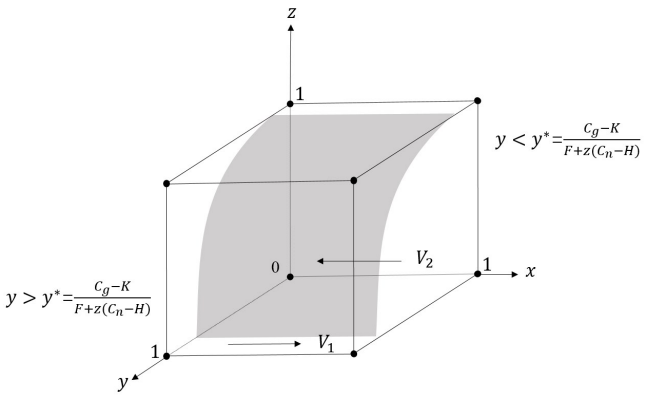


Figure 2. The dynamic evolution of the government's strategic choices.

4.2. Evolutionary Stability Strategies of Digital Platforms

The expected benefit E_y for the digital platform from choosing the "Abuse data" strategy, the expected benefit E_{1-y} for the "Not abuse data" strategy, and the average expected benefit E_p in the game are:

$$\begin{aligned} E_y = {} & xz[(1-e)(1-r)R_1 - C_p - F - \alpha L_p - s] + (1-x)z[(1-e)(1-r)R_1 - C_P - \alpha L_p - s] \\ & + x(1-z)[(1-r)R_1 - C_P - F - \alpha L_p] + (1-x)(1-z)[(1-r)R_1 - C_P - \alpha L_p], \end{aligned} \tag{8}$$

$$\begin{aligned} E_{1-y} = {} & xz[(1-e)(1-r)R_2 - \beta L_p] + (1-x)z[(1-e)(1-r)R_2 - \beta L_p] \\ & + x(1-z)[(1-r)R_2 - \beta L_p] + (1-x)(1-z)[(1-r)R_2 - \beta L_p], \end{aligned} \tag{9}$$

$$E_p = yE_y + (1-y)E_{1-y}. \tag{10}$$

Then the following gives the dynamic equation of the digital platform:

$$F(y) = y(E_y - E_p) = y(y-1)[C_p - (1-ez)(1-r)(R_1 - R_2) + (\alpha - \beta)L_p + xF + zs] \tag{11}$$

taking the derivative with respect to y gives

$$\frac{d(F(y))}{dy} = (2y-1)[C_p - (1-ez)(1-r)(R_1 - R_2) + (\alpha - \beta)L_p + xF + zs]. \tag{12}$$

Putting $F(y) = 0$ so as to get $y = 0, y = 1$ or $x = x^* = -\frac{C_p + (\alpha-\beta)L_p + (1-ez)(1-r)(R_2-R_1) + sz}{F}$, we can see that when $x = x^*$, for any y we have $F(y) = 0$ and $\frac{d(F(y))}{dy} = 0$, so any strategy of the digital platform is a stable strategy. When $x > x^*$, $\frac{d(F(y))}{dy}|_{y=0} < 0$, $\frac{d(F(y))}{dy}|_{y=1} > 0$, and so $y = 0$ is ESS. Conversely, when $x < x^*$, $y = 1$ is ESS.

Based on the above analysis, we can draw a phase diagram to illustrate the dynamic change process of the digital platforms' strategies, as shown in Figure 3. In the figure, $x = x^* = -\frac{C_p + (\alpha-\beta)L_p + (1-ez)(1-r)(R_2-R_1) + sz}{F}$ forms a surface on which any strategy chosen by the platform is stable, while we can see that the surface divides the cubic space into two regions V_3 and V_4. In region V_3, the platforms' strategy will be stable in the "Abuse data" strategy, while in region V_4, the government's strategy is stable in the "Not abuse data" strategy. It can be deduced that the possibility of platforms abusing data is positively correlated with the probability of user claims s and fines F, while being negatively correlated with the profit margin the platform gains from such abuse $(1-r)(R_2 - R_1)$ and the resulting

loss of privacy $(\alpha - \beta)L_p$. Therefore, it is imperative to increase the cost of data abuse by either raising user awareness about the importance of privacy and data protection, empowering them to safeguard their rights. Alternatively, the government may levy targeted data taxes aimed at reducing platform companies' profits derived from personal data abuse. However, there is a tendency for platform companies to invest more in data security technologies to commit more insidious data abuses.

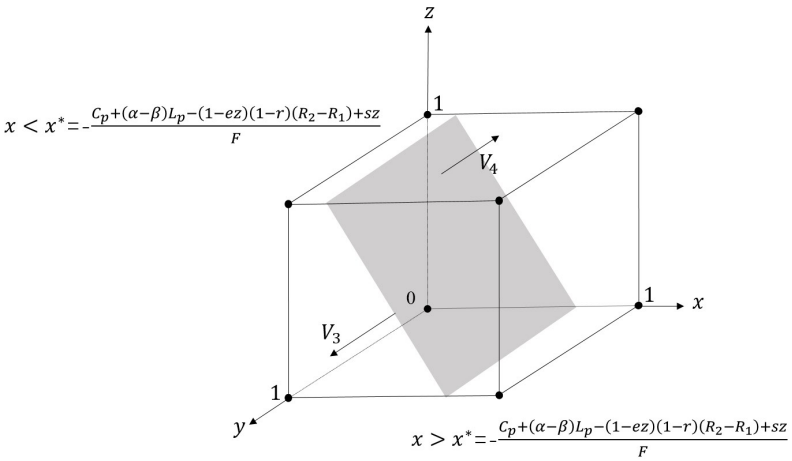


Figure 3. The dynamic evolution of digital platforms' strategic choices.

4.3. Evolutionary Stability Strategies of Users

The expected payoff E_z for users who choose the "Participate in supervision" strategy, the expected payoff E_{1-z} for users who choose the "Not participate in supervision" strategy and the average expected payoff E_u in the game are:

$$\begin{aligned} E_z = {} & xy(U_1 + A - C_u - \alpha L_u + H + s) + (1-x)y(U_1 + A - C_u - \alpha L_u + s) \\ & + x(1-y)(U_2 + A - C_u - \beta L_u) + (1-x)(1-y)(U_2 + A - C_u - \beta L_u), \end{aligned} \tag{13}$$

$$\begin{aligned} E_{1-z} = {} & xy(U_1 - \alpha L_u) + (1-x)y(U_1 - \alpha L_u) + x(1-y)(U_2 - \beta L_u) \\ & + (1-x)(1-y)(U_2 - \beta L_u), \end{aligned} \tag{14}$$

$$E_u = zE_z + (1-z)E_{1-z}. \tag{15}$$

The following gives the user's dynamic equation:

$$F(z) = z(E_z - E_u) = z(1-z)(A - C_u + xyH + ys), \tag{16}$$

taking the derivative with respect to z, we get

$$\frac{d(F(z))}{dz} = (1-2z)(A - C_u + xyH + ys). \tag{17}$$

Supposing $F(z) = 0$ so as to get $z = 0$, $z = 1$ or $y = y^* = \frac{C_u - A}{xH+s}$, it can be seen that when $y = y^*$, for any z with $F(z) = 0$ and $\frac{d(F(z))}{dz} = 0$, any strategy of the users is a stable strategy. When $y < y^*$, $\frac{d(F(z))}{dz}|_{z=0} < 0$, $\frac{d(F(z))}{dz}|_{z=1} > 0$, and so $z = 0$ is ESS. In the remaining case, when $y > y^*$, $z = 1$ is ESS.

Based on the above analysis, we can draw a phase diagram to illustrate the dynamic change process of the users' strategies, as shown in Figure 4.

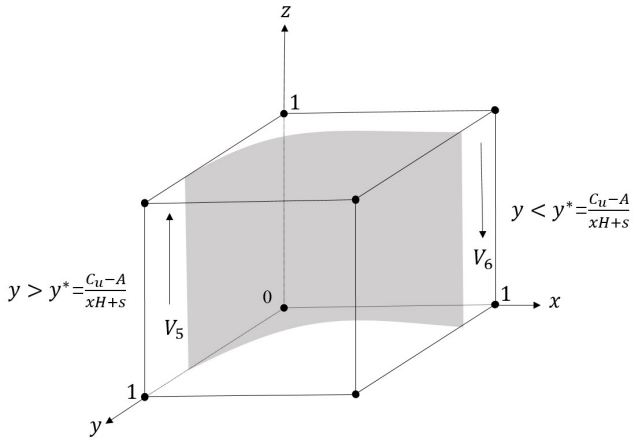


Figure 4. The dynamic evolution of users' strategic choices.

In the figure, $y = y^* = \frac{C_u - A}{xH+s}$ forms a surface on which any strategy chosen by the government is stable, while we can see that the surface divides the cubic space into two regions V_5 and V_6. In region V_5, the users' strategy will be stable in the "Participate in supervision" strategy, while in region V_6, the users' strategy is stable in the "Not participate in supervision" strategy. Our analysis reveals that users' likelihood of participating in supervision is positively associated with government incentives H, compensation s, government's regulation x, and self-satisfaction A, but negatively related to information costs C_u. Users consider the benefits of supervision before deciding to participate and are more likely to participate when government regulation is more prevalent. Therefore, the government should play a mandatory and guiding role in regulation to effectively stimulate users' enthusiasm for participating in supervision.

4.4. Tripartite ESS Analysis

Assembling the equations of Equations (6), (11) and (16), the replication dynamic system of the government, digital platforms and users is obtained. Setting $F(x) = F(y) = F(z) = 0$, yields 14 equilibrium points, including 8 pure strategies $N_1(0,0,0)$, $N_2(1,0,0)$, $N_3(0,1,0)$, $N_4(0,0,1)$, $N_5(1,1,0)$, $N_6(1,0,1)$, $N_7(0,1,1)$, $N_8(1,1,1)$ and 6 mixed strategies (x^*, y^*, z^*). In addition, the stability of the equilibrium point of the replica dynamical system can be judged according to the Liapunov stability discriminant, which means that an equilibrium point such that all eigenvalues of the Jacobi matrix are nonpositive is the ESS of the system. The Jacobi matrix is constructed using Equation (18).

$$J = \begin{bmatrix} \frac{\partial F(x)}{\partial x} & \frac{\partial F(x)}{\partial y} & \frac{\partial F(x)}{\partial z} \\ \frac{\partial F(y)}{\partial x} & \frac{\partial F(y)}{\partial y} & \frac{\partial F(y)}{\partial z} \\ \frac{\partial F(z)}{\partial x} & \frac{\partial F(z))}{\partial y} & \frac{\partial F(z)}{\partial z} \end{bmatrix} \tag{18}$$
$$= \begin{bmatrix} (1-2x)(K - C_g + yF + yzC_n - yzH) & x(1-x)(F + zC_n - zH) & (1-x)y(C_n - H) \\ (y^2 - y)F & (2y-1)[C_p - (1-r)(1-ez)(R_1 - R_2) + (\alpha - \beta)L_p + xF + zs] & (y^2 - y)[s + (1-r)e(R_1 - R_2)] \\ yz(1-z)H & z(1-z)(xH + s) & (1-2z)[A - C_u + y(xH + s)] \end{bmatrix}.$$

The values of the eight pure strategies are put into the Jacobi matrix J to find the eigenvalues of the Jacobi matrix at the different equilibrium points. As shown in Table 5.

It is evident that numerous parameters and complex relationships influence the evolutionary trends of data abuse and its regulation in digital platforms. Hence, to focus on the key issues, the study exclusively focuses on the equilibrium point where digital platforms do not abuse data ($y = 0$), which is divided into two scenarios, as shown in Table 6.

Table 5. Eigenvalues of Jacobi matrix with different equilibrium points.

Equilibrium Points	Eigenvalues
$N_1(0,0,0)$	$\lambda_1^1 = A - C_u$ $\lambda_1^2 = K - C_g$ $\lambda_1^3 = (1-r)\Delta R - C_p - \theta L_p$
$N_2(1,0,0)$	$\lambda_2^1 = A - C_u$ $\lambda_2^2 = C_g - K$ $\lambda_2^3 = (1-r)\Delta R - C_p - \theta L_p - F$
$N_3(0,1,0)$	$\lambda_3^1 = A - C_u + s$ $\lambda_3^2 = F + K - C_g$ $\lambda_3^3 = C_p - (1-r)\Delta R + \theta L_p$
$N_4(0,0,1)$	$\lambda_4^1 = C_u - A$ $\lambda_4^2 = K - C_g$ $\lambda_4^3 = (1-r)(1-e)\Delta R - C_p - \theta L_p - s$
$N_5(1,1,0)$	$\lambda_5^1 = A - C_u + H + s$ $\lambda_5^2 = C_g - F - K$ $\lambda_5^3 = C_p + \theta L_p + F - (1-r)\Delta R$
$N_6(1,0,1)$	$\lambda_6^1 = C_u - A$ $\lambda_6^2 = C_g - K$ $\lambda_6^3 = (1-r)(1-e)\Delta R - C_p - \theta L_p - s - F$
$N_7(0,1,1)$	$\lambda_7^1 = C_u - A - s$ $\lambda_7^2 = C_n - C_g + F + K - H$ $\lambda_7^3 = C_p + \theta L_p + s - (1-r)(1-e)\Delta R$
$N_8(1,1,1)$	$\lambda_8^1 = C_u - A - s - H$ $\lambda_8^2 = C_g - C_n - F - K + H$ $\lambda_8^3 = C_p + \theta L_p + s + F - (1-r)(1-e)\Delta R$
(x^*, y^*, z^*)	Saddle Point

(i) $\Delta R = R_1 - R_2, \quad \Delta R > 0, \quad \theta = \alpha - \beta, \quad \theta > 0$; (ii) Evolutionary stable strategies (ESS) appear only in pure strategies [47], so mixed strategies (x^*, y^*, z^*) are excluded first.

Table 6. Determination of stable equilibrium point.

Scenario	ESSs	Required Conditions
Government has no regulatory motivation	$N_1(0,0,0)$ is the only ESS	$A < C_u$ $K < C_g$ $\Delta R < \frac{C_p + \theta L_p}{1-r}$
	$N_1(0,0,1)$ is the only ESS	$A > C_u$ $K < C_g$ $\Delta R < \frac{F + C_p + \theta L_p}{1-r}$
Government has regulatory motivation	$N_1(1,0,0)$ is the only ESS	$A < C_u$ $K > C_g$ $\Delta R < \frac{C_p + \theta L_p + s}{(1-r)(1-e)}$
	$N_1(1,0,1)$ is the only ESS	$A > C_u$ $K > C_g$ $\Delta R < \frac{F + C_p + \theta L_p + s}{(1-r)(1-e)}$

(i) $\Delta R = R_1 - R_2, \quad \Delta R > 0, \quad \theta = \alpha - \beta, \quad \theta > 0$; (ii) Evolutionary stable strategies (ESS) appear only in pure strategies [47], so mixed strategies (x^*, y^*, z^*) are excluded first.

Based on the above analysis, Propositions 1 to 2 can be posited.

Proposition 1. *When $K < C_g$, there exist two possible ESS points, $N_1(0,0,0)$ and $N_4(0,0,1)$. When $A < C_u$, $\Delta R < \frac{C_p + \theta L_p}{(1-r)}$, that is, $r \in [1 - \frac{C_p + \theta L_p}{\Delta R}, 1]$, and so $N_1(0,0,0)$ is the only ESS point where the government does not regulate digital platforms, platforms do not abuse data, and users do not participate in supervision. When $A > C_u$, $\Delta R < \frac{C_p + \theta L_p + s}{(1-r)(1-e)}$ and $e \in [1 - \frac{C_p + \theta L_p + s}{(1-r)\Delta R}, 1]$, $N_4(0,0,1)$ is the only ESS where the government does not supervise digital platforms, platforms do not abuse data, and users participate in supervision.*

Proof. When $A < C_u$, $K < C_g$ and $\Delta R < \frac{C_p + \theta L_p}{(1-r)}$, we can get $\lambda_2^2 > 0, \lambda_4^1 > 0, \lambda_6^2 > 0$, that is $N_2(1,0,0)$, $N_4(0,0,1)$ and $N_6(1,0,1)$ are not the ESSs, and $\lambda_1^1 < 0, \lambda_1^2 < 0, \lambda_1^3 < 0$,

so $N_1(0,0,0)$ is the only ESS. When $A > C_u$, $K < C_g$ and $\Delta R < \frac{C_p+\theta L_p+s}{(1-r)(1-e)}$, we can get $\lambda_1^1 > 0, \lambda_2^1 > 0, \lambda_6^2 > 0$, that is $N_1(0,0,0)$, $N_2(1,0,0)$ and $N_6(1,0,1)$ are not the ESSs, and $\lambda_4^1 < 0, \lambda_4^2 < 0, \lambda_4^3 < 0$, so $N_4(0,0,1)$ is the only ESS. □

Proposition 1 indicates that when the government has no incentive to supervise (i.e., the costs of regulation outweigh the benefits of regulation $K < C_g$), there are two ways to prevent data abuse. One is to adjust the tax rate. According to the general principles of economics, an increase in the tax rate will inhibit enterprises from expanding their business, and in the case of a high tax rate, if platforms still insist on abusing data, most of the revenue will be collected by the government. When the costs outweigh the benefits, platforms often have no incentive to abuse data. For example, France passed a set of digital services tax (DST) rules in 2019 that imposes a 3% tax on digital platforms with over €25 million in annual taxable income [49]. This approach increases the tax burden on platform businesses that abuse user data and promotes a fairer distribution of tax responsibilities. It serves as an example for other governments and regulators to curb data abuse by digital platforms through tax policies. The other is to rely on leveraging user self-efficacy and enhancing the perceived value of private data. A "free-rider" condition can be achieved when the user increases the probability of refusing to provide data to the platform. Under this stabilization strategy, the government's optimal decision is not to supervise.

Proposition 2. *When $K > C_g$, there are two possible ESS points, $N_2(1,0,0)$ and $N_6(1,0,1)$. When $A < C_u$, $\Delta R < \frac{F+C_p+\theta L_p}{1-r}$, that is, $F \in [(1-r)\Delta R - C_p - \theta L_p, \infty]$, $N_2(1,0,0)$ is the only ESS: the government supervises the digital platforms, platforms do not commit data abuse, and users do not participate in supervision. When $A > C_u$, $\Delta R < \frac{F+C_p+\theta L_p+s}{(1-r)(1-e)}$, that is, $F \in [(1-r)(1-e)\Delta R - C_p - s - \theta L_p, \infty]$, $N_6(1,0,1)$ is the only ESS: the government supervises the digital platforms, platforms do not commit data abuse, and users participate in supervision.*

Proof. When $A < C_u$, $K > C_g$ and $\Delta R < \frac{F+C_p+\theta L_p}{1-r}$, we can get $\lambda_1^2 > 0, \lambda_4^2 > 0, \lambda_6^1 > 0$, that is $N_1(0,0,0)$, $N_4(0,0,1)$ and $N_6(1,0,1)$ are not the ESSs, and $\lambda_2^1 < 0, \lambda_2^2 < 0, \lambda_3^3 < 0$, so $N_2(1,0,0)$ is the only ESS. When $A > C_u$, $K > C_g$ and $\Delta R < \frac{F+C_p+\theta L_p+s}{(1-r)(1-e)}$, we can get $\lambda_1^1 > 0, \lambda_2^1 > 0, \lambda_4^2 > 0$, that is $N_1(0,0,0)$, $N_2(1,0,0)$ and $N_4(0,0,1)$ are not the ESSs, and $\lambda_6^1 < 0, \lambda_6^2 < 0, \lambda_6^3 < 0$, so $N_6(1,0,1)$ is the only ESS. □

Proposition 2 shows that when the government is motivated to supervise (i.e., benefits of regulation outweigh the the costs of regulation $K > C_g$), it can maintain the existing tax rate on the one hand, and can effectively deter digital platform companies from committing data abuse by increasing the penalty F so that it is greater than the net increase in profits from the platform's data abuse and covers the additional loss from a privacy breach. This is well documented in practice. For example, in the case of Facebook's abuse of user data, the U.S. Department of Justice, the Federal Trade Commission and Facebook reached a 20-year settlement agreement on protecting user privacy, the main elements of which include Facebook paying a 5 billion dollar fine and accepting further regulation by the Federal Trade Commission. In addition, the SEC reached an administrative settlement over allegations that Facebook failed to adequately disclose the risk of user data misuse and required the company to pay a 100 million dollar fine to the SEC. These penalties serve as a striking testament to the importance of strict and rigorous oversight, as well as the vital role that fines play in incentivizing compliance with established best practices in data management. Proposition 2 further reveals that the difference in ΔR between the stable points of user participation (1,0,1) and non-participation (1,0,0) is $\frac{-e(F+C_p+\theta L_p)-s}{(1-r)(1-e)} < 0$. This implies that, on one hand, a larger number of users participating in data abuse results in fewer additional benefits due to negative network externalities, which decreases the platform's incentive for data abuse. On the other hand, user participation in supervision can effectively address information asymmetry and improve the efficiency of government regulation. To imple-

ment this framework in practice, we suggest creating additional user supervision channels to lower costs and enhancing users' privacy awareness to increase their satisfaction with supervision. This will encourage more active participation in supervision and ultimately achieve a successful dual regulatory system.

Summarizing Propositions 1 and 2, this study yields two corollaries.

Corollary 1. *Both governments and users have measures with which to curb data abuse by digital platforms.*

Whether the government chooses to regulate or not, the government can prevent the abuse of data by digital platforms through effective policy controls, which can set high penalties in a regulatory scenario or high tax rates in a non-regulatory scenario. High penalties are a huge pressure for digital platforms, which can force them to handle user data more cautiously and defend user privacy. Users can weaken the incentive for digital platforms to abuse data by refusing to provide data in a supervised context, and increase the incentive to claim to compress the profit margin of platforms. The backlash from users has forced platform companies to seek more sustainable business models, reduce their reliance on user data, and thereby reduce instances of data abuse. These findings can help governments make flexible choices based on how fines are actually implemented, how easily tax rates are adjusted, and the users' perceived value of privacy.

Corollary 2. *The risk of privacy breaches gives digital platforms a recurring incentive to abuse data.*

With the improvement of data security technology, there is a possibility of recurrence of data abuse by digital platforms. Because of the existence of the risk of privacy leakage, platform companies can commit data abuse if they increase their investment in privacy protection so as to reduce the risk of an additional privacy leakage of the platform. At this point, it is necessary to weigh the relationship between the benefits of data abuse and the investment cost of privacy protection, when the technology advances to the point that only a small cost is needed to significantly reduce the privacy leakage risk, and the government tax rate r and penalty F remain unchanged, the platforms have an incentive to engage in data abuse again. Companies such as Google, Facebook, and Alibaba have faced numerous allegations of data abuse. Based on the findings of this study, it is plausible that they are continuously reducing privacy risks caused by data breaches, evading standard monitoring methods by users and governments, and resorting to more covert means of carrying out data misuse. Therefore, relevant government regulatory policies should focus on the efficiency and cost of data security technologies for timely adjustment, so as to achieve the elimination of repeated violations.

5. Numerical Simulation

In this section, numerical simulation will be used to characterize the evolution path and analyze the sensitivity of the model, and MATLAB will be used to simulate the changes of the stability strategy under different scenarios and verify the equilibrium stability conclusion. In the simulation process, parameter values are based on an analysis of widely publicized digital platform data abuse penalty cases across several countries, such as the case where Didi was fined 8 billion RMB [50], Facebook's violation of GDPR [51], and TikTok's violation of the U.S. Children's Online Privacy Protection Act [52], etc.

Also, the parameters are set according to the following principles: (1) The value gap between variables is in alignment with reality, such as: (i) Referring to the case of Didi being punished, as shown in Table 7, the ratio of ΔR to F is about 3.00:0.80 under the government's regulation. (ii) Taking China as an example, the corporate income tax rate is 25%, of which there is a 10% tax rate discount for high-tech enterprises, and so $r \in [0.15, 0.25]$. (iii) The value added of revenue from the platform's data abuse is composed of online marketing technology services, transaction services and merchandise sales, of which merchandise sales account for about 23%. Referring to the case of "User v. Platform big data killing", the user's claim is "One refund and three compensation", and the ratio of ΔR to s is about $3.00 : 0.21$. (iv) The technical cost of data abuse by the platform is characterised by the enterprise's R&D investment, resulting in the ratio of ΔR to C_p being established at $3.00 : 0.9$. (2) The parameter values in each case follow the propositional constraints

in Section 3. (3) When the ESS changes, the change of parameter values should be as small as possible to avoid the emergence of extreme numbers and facilitate the subsequent parameter sensitivity analysis.

Table 7. The case of Didi being punished.

Item	2021	2020	2019
Revenue	1738.27	1417.36	1547.86
Rate	3.45%	2.78%	0.34%
R&D	94	63	53
Penalty	80.26	-	-
Goodwill decrement	28	-	-

Data source: Didi IPO files. The unit of revenue, R&D, penalty and goodwill decrement is 100 billion yuan.

Combining the above practical cases and the stability analysis of the equilibrium point, This study examines four scenarios, each one with its specific setting of the parameters of the model, as shown in Table 8.

Table 8. Parameter settings for the effect of initial probability on evolutionary results.

Parameters	Case 1	Case 2	Case 3	Case 4
A	0.50	0.50	1.00	1.00
C_u	1.00	1.00	0.50	0.50
K	0.80	1.00	0.80	0.80
C_g	1.00	0.80	1.00	0.50
ΔR	3.00	3.00	3.00	3.00
θ	0.60	0.10	0.30	0.10
L_p	2.50	2.50	2.50	2.50
F	0.80	0.80	0.80	0.80
e	0.10	0.10	0.10	0.10
s	0.21	0.21	0.21	0.21
r	0.25	0.25	0.25	0.25
C_p	0.90	0.90	0.80	0.90
H	0.10	0.10	0.10	0.10
C_n	0.28	0.28	0.28	0.28

5.1. Effect of Initial Probability on Evolutionary Paths

The results of the stabilization strategies of the government, digital platforms, and users, under different scenarios with different initial probabilities, x, y, z take the values of $0.2, 0.5, 0.8$ respectively, are shown in Figure 5.

We can see the following in Figure 5: (a) When $A < C_u$, $K < C_g$ and $\Delta R < \frac{C_p+\theta L_p}{(1-r)}$, whatever the initial values of x, y and z, eventually converge to 0. (b) When $A < C_u$, $K > C_g$ and $\Delta R < \frac{F+C_p+\theta L_p}{1-r}$, regardless of the initial values of x, y and z, the values of x eventually converge to 1, while the values of y, z converge to 0. (c) When $A > C_u$, $K < C_g$ and $\Delta R < \frac{C_p+\theta L_p+s}{(1-r)(1-e)}$, it does not matter what the initial values of x, y and z are, the values of x and y eventually converge to 0, while the values of z converge to 1. (d) When $A > C_u$, $\Delta R < \frac{F+C_p+\theta L_p+s}{(1-r)(1-e)}$, regardless of the initial values of x, y and z, the values of x and z eventually converge to 1, while the values of y converge to 0. So, it can be seen that the initial probability does not affect the subjects' choices of strategy, but has a significant effect on the time required to reach equilibrium.

The specific analysis is as follows.

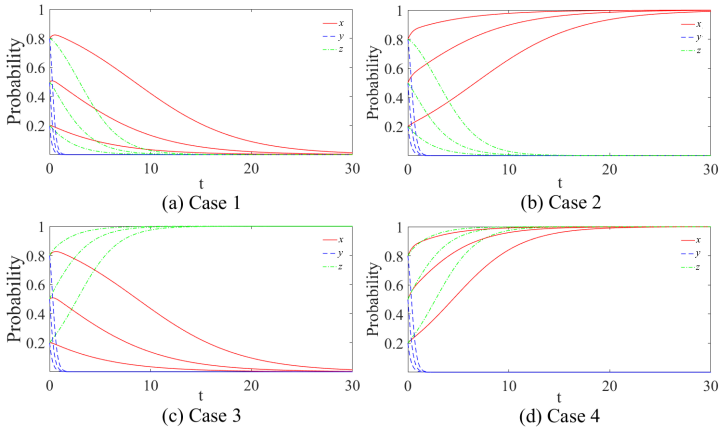


Figure 5. Evolutionary trends in different scenarios. (**a**) $A < C_u$, $K < C_g$ and $\Delta R < \frac{C_p+\theta L_p}{(1-r)}$; (**b**) $A < C_u$, $K > C_g$ and $\Delta R < \frac{F+C_p+\theta L_p}{1-r}$; (**c**) $A > C_u$, $K < C_g$ and $\Delta R < \frac{C_p+\theta L_p+s}{(1-r)(1-e)}$; (**d**) $A > C_u$, $\Delta R < \frac{F+C_p+\theta L_p+s}{(1-r)(1-e)}$.

(1) Government. Observing (b) and (d) in Figure 5, we can see that the stronger the initial willingness of the government to supervise, the shorter it takes to reach the steady state of "Supervise" (the closer the initial value of x is to 1, the faster it converges to (1), which is in line with the actual situation. Observing (a) and (c) in Figure 5, the x curve has a brief process of rising and then falling, mainly because the government is torn between the regulatory costs and social benefits involved in choices. When the government does not consider the interests of users, the regulatory costs will decrease in terms of government reputation cost and the burden of incentivizing user participation in supervision. This makes it easy for K to exceed the threshold needed to meet the condition of C_g, and government regulation will reach a stable equilibrium more quickly. Observing (b) and (c) in Figure 5, in the case of users' participation in supervision, because users can provide the government with effective information about the digital platforms and reduce the information asymmetry in the regulatory process, which greatly reduces the cost of government supervision, so that the stronger the initial willingness of government supervision, the shorter the time required to reach the steady-state strategy of "Supervise" (the closer the initial value of x is to 0, the faster it converges to 0).

(2) Digital platforms. Observing Figure 5, it becomes apparent that when the initial willingness of platforms to abuse data is stronger, the faster one reaches the steady-state strategy of "Not abuse data". This is attributed to the fact that enterprises are primarily motivated by maximizing efficiency and profits, and when they try one strategy and fail to deliver desired outcomes, they will quickly choose another strategy that is more beneficial, while when the initial willingness of the platform to commit data abuse is low, enterprises will be stuck in a tangle for a long time, resulting in a longer time required to reach steady state. Meanwhile, comparing (c) with (a), (b), and (d) in Figure 5, it can be seen that it takes longer for digital platforms to reach steady state when only users supervise the situation. The reason for this is that a single constraint by users is less of a deterrent to platforms than a single government supervision or dual user-government supervision, so in practice, the government still has the dominant role in supervising data abuse by platforms.

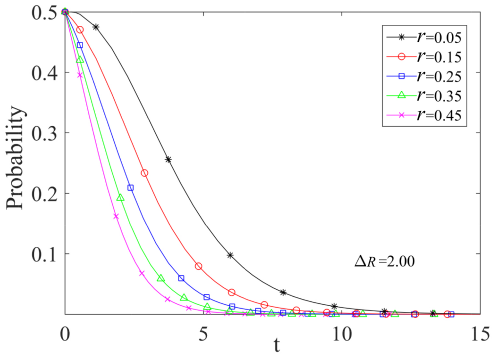
(3) Users. Observing Figure 5, similar to the case of the government, we can obtain similar conclusions; that is, the stronger the initial willingness of the users, the shorter the time required to reach the stabilization strategy. In the case that x converges to 0, the closer x is to 0, the less time required to evolve to the "Not participate in supervision" stabilization strategy. In the case that x converges to 1, the closer x is to 1, the less time it takes to evolve to the "Participate in supervision" stabilization strategy. This finding emphasizes the importance of user initiative.

5.2. Sensitivity Analysis

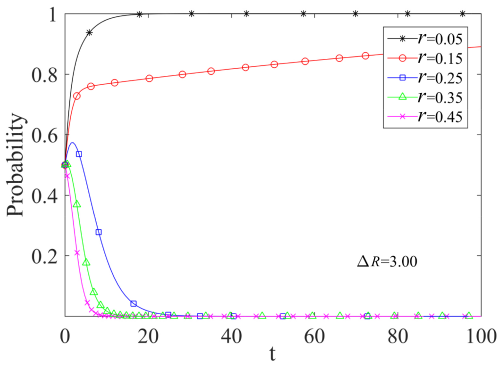
This section focuses on how to optimize the parameters to improve the probability of digital platforms not abusing data. Based on the case study, considering that the data has a typical scale effect, platforms with larger volumes of data tend to generate higher profits through data abuse. Therefore, this paper divides digital platforms into two categories, one is small digital platforms with small scale data, and the increase in revenue obtained by relying on data abuse is less ($R = 2.00$); the other is large digital platforms with larger volumes of data, such as Didi, Facebook, etc., and the increase in revenue from data abuse is large ($R = 3.00$). Meanwhile, the parameters of Case2 are used as the assignment benchmark, and the initial probabilities of x, y, and z are set to 0.50 for numerical simulation. The specific analysis is as follows.

(1) The tax rate paid by the platform

Keeping the other parameters constant, let r increase in increments of 0.10 in the interval $[0.05, 0.45]$, as shown in Figure 6. Overall, as r decreases, i.e., as tax incentives for platforms increase, the rate at which governments and platforms converge on a stabilization strategy continues to increase. For small digital platforms, the change in tax rate does not affect the ultimate stabilization strategy of platforms, due to the small benefits from data abuse, which are "Not abuse data". While for large digital platforms, due to the scale effect, the benefits from data abuse are higher and the larger tax incentives ($r < 15\%$) increase the incentive for the platform to abuse data, which will eventually stabilize the "Abuse data" strategy.



(a) Evolution of small digital platforms' behaviors



(b) Evolution of large digital platforms' behaviors

Figure 6. The Effect of different tax rates on the evolutionary process (r).

Therefore, for platforms of different data sizes, the government can try to formulate tiered tax policies to ensure the vitality of the enterprises while effectively reducing their incentive to abuse of data. As exemplified by Didi Global Inc., the tax rates for the company in the three years prior to the data scandal were 3.45% (2021), 2.78% (2020), and 0.34% (2019). The company benefited from significant tax incentives in China, which enabled it to accumulate capital quickly and further incentivized the misuse of data to increase profits.

(2) Amount of penalties faced for data abuse committed by digital platforms

Let F increase with 0.40 at unit increments. The results are shown in Figure 7. On the whole, the time shortening caused by the unit increment decreases with an increase of F, showing the characteristic of marginal decrease. Observing Figure 7a,d, we can see that for small digital platforms, the change of F only affects the time to reach equilibrium without affecting the resulting final stabilization strategy. For large digital platforms, the change in F not only affects the time to reach equilibrium but also affects the final stabilization strategy, and when the government penalty is set in a low range (as shown in the figure, $F < 0.45$), the platform can still obtain a larger gain after paying the penalty. This is the main reason why large platforms ignore government supervision and commit violations in practice. Looking at Figure 7b,e, the change in F does not affect the final outcome of the government's strategy, but since fines are another major fiscal revenue source of the government besides taxes, the increase in revenue will certainly help the government to intervene in supervision faster. Similarly, Figure 7c,f show that penalties have no effect on users' final choice of strategy, but as F increases, it takes longer for users to reach a stable state of participation in supervision.

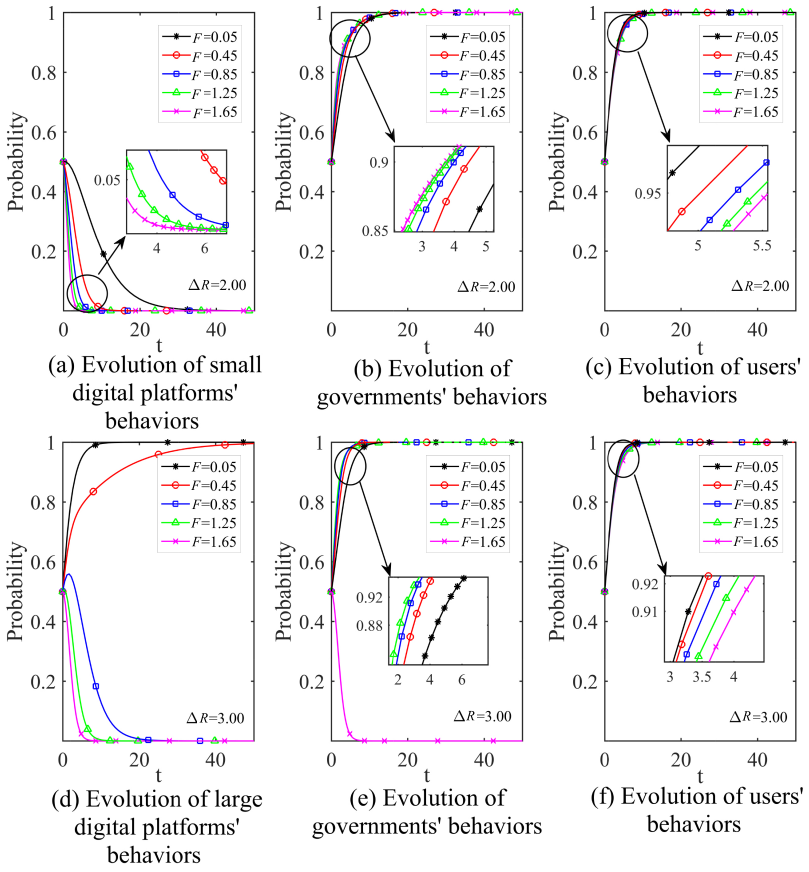
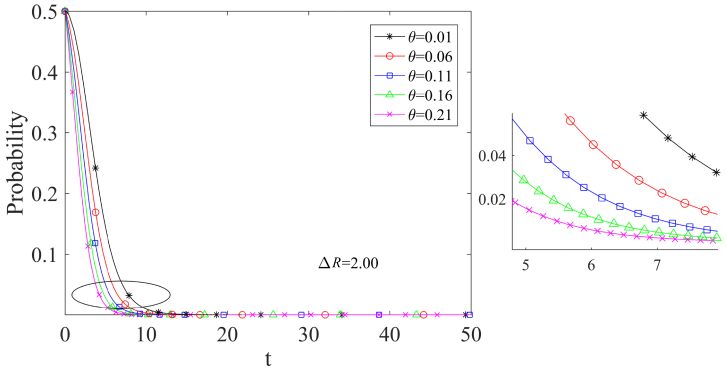


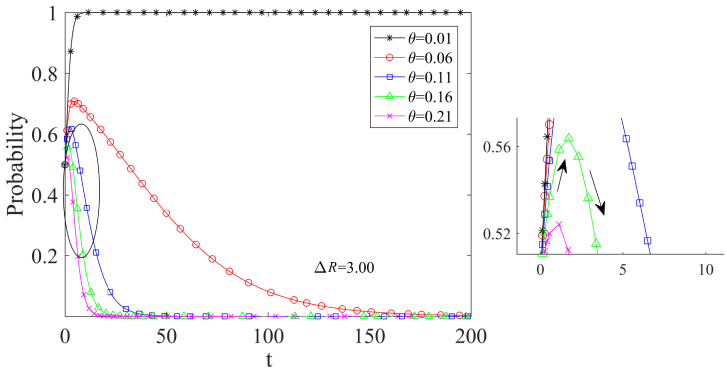
Figure 7. The Effect of different sizes of penalties on the evolutionary process (F).

(3) Incremental risk of privacy breach

Let θ begin with 5% and increase with a unit increment. The evolutionary process is shown in Figure 8, which leads to similar conclusions as for the tax rate and penalty; that is, for small digital platforms, the incremental risk of privacy breach does not affect the evolutionary stability strategy. However, for large digital platforms, a lower privacy risk increment (as shown in Figure 8b, when $\theta = 0.01$) will stabilize the platform in the state of committing data abuse ($y = 1$). Moreover, observing Figure 8b, we can see that when $\theta > 0.06$, there is a brief rise and then decline in the probability of committing data abuse at the beginning of the platform's evolution, mainly because the platform tries to increase its technical investment in data protection to reduce the privacy loss from committing data abuse. Furthermore, choosing $t = 5$, we can see that as θ decreases, the value of the probability becomes larger, indicating that platforms with advanced data protection technologies are more likely to abuse data and more covert violations in the same period. The results indicate that improved technological capabilities can create pressure for platform companies to collect more user data and also increase the value of data, making it easier for them to succumb to the temptation of data abuse. For instance, Amazon was found to be using third-party seller data to develop its own competitive products, leveraging its advanced technological capabilities to access and analyze the data. Therefore, even though platforms may improve their data protection technologies to reduce the risk of privacy breaches, the pressure and temptation to abuse data remains high.



(a) Evolution of small digital platforms' behaviors



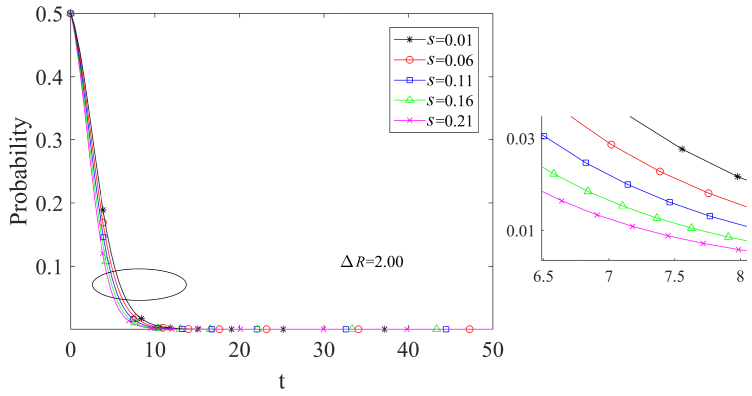
(b) Evolution of large digital platforms' behaviors

Figure 8. Effect of different privacy risk increments on the evolutionary process ($\theta = \alpha - \beta$).

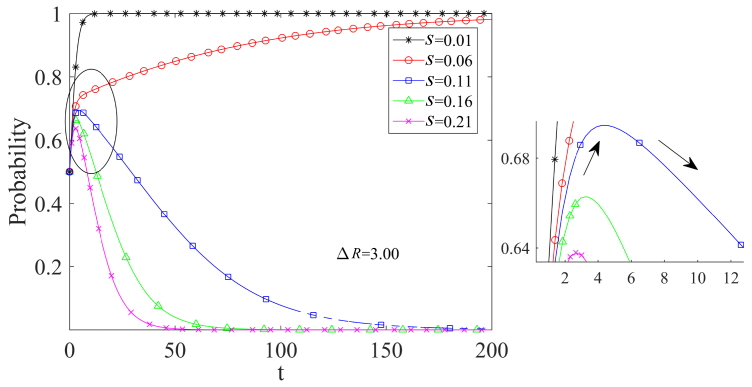
(4) Probability of users' claiming compensation

Let s increase by increments of 5%, then we get the evolution process in Figure 9. For platforms, the larger s is, the faster it reaches ESS. In particular, as in (b) in Figure 9, for large platforms, when the value of s is high ($s > 11\%$), its evolution at the beginning has a short rise and then a fall, because in the short term, the platform tries to rely on some PR ability to mitigate the loss. And it is clear that there is a range of values for s

(11% $< s <$ 6%) in the large platform where no equilibrium solution exists. It can be seen that user participation may lead to even greater system instability. But in the long term, there is an obvious negative externality in the proportion of user claims, for which reason the gains from data abuse cannot offset the corresponding losses (such as penalties, loss of user data, etc.). Therefore, the government should actively guide users to defend their rights, open up complaint channels, and increase the proportion of user claims to effectively stop data abuse by platforms.



(a) Evolution of small digital platforms' behaviors



(b) Evolution of large digital platforms' behaviors

Figure 9. The impact of different probabilities of users' claiming compensation on the evolutionary process (s).

(5) Government's rewards for users

As shown in Figure 10, a change in the value of H significantly affects the choice of strategy by large digital platforms, the government, and users. The larger H is, the greater the financial burden on the government and the longer it takes for the government to stabilize its regulatory strategy. Further, when H is larger than H' (a certain critical value), the government cannot afford the high cost of rewards, and the government will tend to choose not to supervise. At the same time, the government's rewards to users have negative externalities, and as the value of H increases, this makes the regulatory efficiency and user incentives put the cart before the horse, and platforms have the opportunity to abuse data.

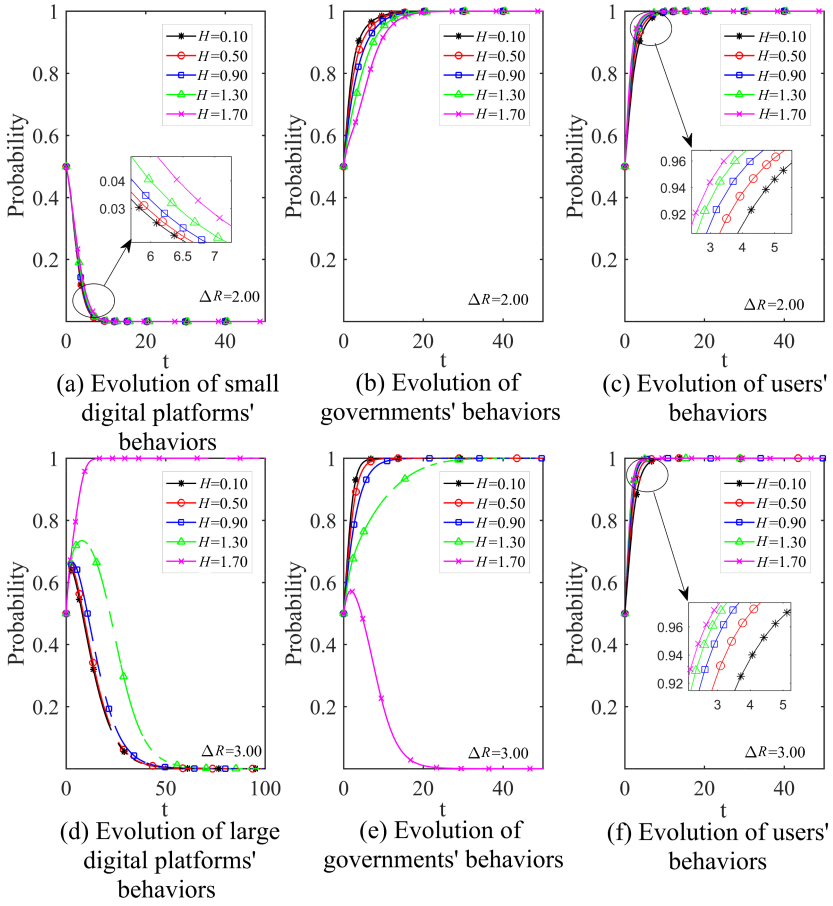


Figure 10. The impact of different government's rewards for users on the evolutionary process (H).

6. Discussion

This study constructed a model which was a tripartite evolutionary game to explore the governance mechanism of data abuse in digital platforms, focusing on tax policies, penalties, privacy leakage risks, and user claims for compensation. Through this study, we have identified critical factors that influence platforms' decisions to engage in data abuse. Whether platforms choose to abuse data depends on the interplay between the incremental revenue, technological costs, privacy breaches, reputation costs, and the losses incurred from government and user punishments. By employing evolutionary game theory, we have identified four ways in which platforms can refrain from engaging in data abuse, which are divided into two categories: government with regulatory motives and government without regulatory motives. Furthermore, we extracted simulation parameters from typical cases and used MATLAB software to conduct a sensitivity analysis on key factors, such as how higher tax incentives ($r < 15\%$) and lower penalties ($F < 0.45$) can reduce the motivation of data abuse by small digital platforms, but fail for large digital platforms. Additionally, by analyzing the pressure and temptation to improve the technological capabilities of platform companies, we found that the existence of privacy leakage risks creates recurring incentives for digital platforms to engage in data abuse. Relevant regulatory policies should therefore focus on promptly adjusting the efficiency and costs of data security technologies to eliminate repeated violations.

6.1. Main Contributions

The main contribution of this study is reflected in two aspects: the contribution to theory and the significance to practice.

From a theoretical perspective, unlike previous research on data abuse [16,53,54], this study explores regulatory issues of data abuse by considering the collaborative behavior

of the government, platform, and users. A new research perspective is presented based on mathematical model deduction. Based on the theory of opportunity and motivation, combined with theoretical derivation and simulation results, we believe that the basic method to govern data abuse by digital platforms lies in reducing their motivation and compressing their opportunity space. On the one hand, the motivation of digital platforms to abuse data comes from the illegal profits obtained from this illegal operation. On the other hand, users' participation in supervision can reduce the information asymmetry in the process of data abuse by platforms and reduce the government's supervision costs. From using the evolutionary game as a model, it can be seen that the motivation of users to participate in supervision is influenced by the users' personal self-efficacy, government incentives, platform compensation, etc.

The study also has significant practical implications for government policy formulation, platform strategy choice, and the protection of users' rights. From a government perspective, the research provides insights into the behavior and motivations of platform companies, aiding in the formulation of more precise regulatory policies and taxation systems to reduce data misuse. Additionally, evolutionary game research can help the government evaluate policy effectiveness and make timely adjustments. For platform enterprises, the study can increase their understanding of the costs and risks of data misuse, thereby promoting long-term development. Finally, for users, the research helps them understand the costs and risks of data abuse by platform companies, their status and rights within the regulatory mechanism, and enhances their awareness and ability to protect their rights and interests.

6.2. Recommendation for Government

In order to provide the government with precise insights into governance, we have first specified the revenue composition of the government within the context of gaming. As demonstrated in Section 2, the government's return primarily derives from taxes and fines levied on the platform. Additionally, our model is based on the government considering user interests and allowing users to receive supervised rewards. However, if the government does not consider this point and only focuses on its own fines and tax revenues, it will lead to two results. The first result is that the government will implement high-intensity regulation to obtain fines, which will stifle the development of platform enterprises. The second result is that the government will implement low-intensity regulation to obtain high tax revenues, which will lead to data abuse and industry disorder, causing great harm to user rights and interests. Therefore, government decisions will be influenced by platform and consumer decisions. In summary of our research analysis and findings, we propose the following management recommendations.

From a regulatory framework perspective, it is recommended that the government encourage user participation and establish a dual regulatory framework. User involvement in supervision can reduce the information asymmetry and reduce government regulatory costs. Evolutionary game theory models reveal that user participation in supervision is influenced by factors such as personal self-efficacy, government incentives, and platform compensation. When a user's self-efficacy is much higher than the information cost required to participate in supervision, the user evolves to a stable state of participation. As the claim ratio of users continues to rise, the profit margin for platform abusing data is constantly compressed, and the opportunities for violations continue to decrease. Therefore, from a social perspective, the harm of data abuse needs to be emphasized to enhance users' self-efficacy, while from the government perspective, a suitable incentive limit needs to be set to actively guide users' rights protection and to provide them with accessible complaint channels, thus reducing the opportunities for platform data abuse.

From a regulatory policy perspective, it is recommended that the government try to formulate tiered tax policies and dynamic penalty amounts for platforms of different data scales. Sensitivity analysis reveals that for large-scale digital platforms, due to the existence of economies of scale, the profits generated by data abuse are higher, and higher

tax incentives (r < 15%) increase the motivation for abusing data. Therefore, for platforms of different data scales, the government can try to formulate tiered tax policies to protect the vitality of enterprise innovation and effectively reduce the motivation for data abuse. This has strong practical significance, and for small platform enterprises, it is recommended to maintain certain tax incentives, such as China's 10% tax rate incentive policy for high-tech Internet companies. For large platform enterprises, it may be necessary to consider increasing tax rates or adjusting value-added tax structures, such as implementing digital taxes on large-scale data-driven platforms.

From a technical adoption perspective, it is recommended that the government adopt more advanced data security technologies, such as AI, blockchain and differential privacy, to construct a more agile data abuse regulatory network. Our research shows that platforms with advanced data protection technologies are more likely to engage in data abuse and that their improper behavior is more secretive. As Milkalef P. et al. [55] pointed out, the application of artificial intelligence technology has a significant role in improving the performance of government organizations. Therefore, as platforms have incentives to increase their investment in data protection to reduce privacy risks, the government needs to pay attention to the application of cutting-edge data protection (security) technologies and the development of platform businesses with high-end data protection technologies and facilities in order to monitor platform data usage behavior from a technical perspective.

6.3. Limitation and Future Research

The focus of this study is on the construction of a data abuse analysis framework and an evolutionary game analysis model involving three main actors. The study analyzes the key factors that affect the implementation of data abuse by platforms at a theoretical level and explores the regulatory mechanisms. However, there are certain limitations to this study. Firstly, in terms of model construction, we assumed that all actors have bounded rationality and that the government and platform consider reputation costs, which may differ from the actual situation. Future research could consider different risk tendencies of the actors (such as risk aversion, risk-seeking, and risk neutrality) to further explore this issue. Secondly, in terms of model effectiveness, although we used sensitivity analysis to simulate the model's development with the actual situation, we cannot judge its effectiveness. Future research could consider using system dynamics methods to model this problem and further compare the differences between the two methods. In addition, this study does not involve empirical research, which limits its practical expansion to a certain extent. In the future, it can be combined with empirical data analysis methods to verify the conclusions of this study and enrich its methods. Based on this study, there are some directions that can be expanded in the future. For example, behavioral economics has attracted the attention of many scholars in management, and future research could consider the impact of platform operators' behaviors on decision-making, such as risk aversion, overconfidence, altruism, and fairness awareness behaviors.

Author Contributions: Conceptualization, Z.W., C.Y. and X.L.; methodology, Z.W.; software, Z.W. writing—original draft preparation, Z.W.; writing—review and editing, C.Y. and X.L.; supervision, C.Y.; project administration, X.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available on request from the corresponding author.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

ESS	Evolutionary Stability Strategies
Didi	DiDi Global Inc.

References

1. Ichihashi, S. Competing data intermediaries. *RAND J. Econ.* **2021**, *52*, 515–537. [CrossRef]
2. Ichihashi, S.; Kim, B.C. Addictive Platforms. *Manag. Sci.* **2022**, *69*, 1127–1145. [CrossRef]
3. Zhu, Y.; Grover, V. Privacy in the sharing economy: Why don't users disclose their negative experiences? *Int. J. Inf. Manag.* **2022**, *67*, 102543. [CrossRef]
4. Just, N. Governing online platforms: Competition policy in times of platformization. *Telecommun. Policy* **2018**, *42*, 386–394. [CrossRef]
5. Belleflamme, P.; Peitz, M. Managing competition on a two-sided platform. *J. Econ. Manag. Strategy* **2019**, *28*, 5–22. [CrossRef]
6. Teh, T.H. Platform governance. *Am. Econ. J. Microecon.* **2022**, *14*, 213–254. [CrossRef]
7. Graef, I. When data evolves into market power: Data concentration and data abuse under competition law. In *Digital Dominance*; Moore, M., Tambini, D., Eds.; Oxford University Press: Oxford, UK, 2018; pp. 71–97.
8. Mousavi, R.; Chen, R.; Kim, D.J.; Chen, K. Effectiveness of privacy assurance mechanisms in users' privacy protection on social networking sites from the perspective of protection motivation theory. *Decis. Support Syst.* **2020**, *135*, 113323. [CrossRef]
9. Rochet, J.C.; Tirole, J. Platform competition in two-sided markets. *J. Eur. Econ. Assoc.* **2003**, *1*, 990–1029. [CrossRef]
10. Gawer, A.; Cusumano, M.A. Industry platforms and ecosystem innovation. *J. Prod. Innov. Manag.* **2014**, *31*, 417–433. [CrossRef]
11. Parker, G.G.; Van Alstyne, M.W.; Choudary, S.P. *Platform Revolution: How Networked Markets Are Transforming the Economy and How to Make them Work for You*; WW Norton & Company : New York, NY, USA, 2016.
12. SAT, C. Notice on Issues Related to Enterprise Income Tax Preferential Policies for Software and Integrated Circuit Industry. 2016. Available online: http://www.chinatax.gov.cn/chinatax/n810341/n810755/c2128416/content.html (accessed on 15 December 2022).
13. Cloarec, J. The personalization–privacy paradox in the attention economy. *Technol. Forecast. Soc. Chang.* **2020**, *161*, 120299. [CrossRef]
14. Fainmesser, I.P.; Galeotti, A.; Momot, R. Digital privacy. *Manag. Sci.* **2022**, *Epub ahead of print*. [CrossRef]
15. Wang, W.; Huang, H.; Yin, Z.; Gadekallu, T.R.; Alazab, M.; Su, C. Smart contract token-based privacy-preserving access control system for industrial Internet of Things. *Digit. Commun. Netw.* **2022**, *in press, Corrected Proof*. [CrossRef]
16. Liu, W.; Long, S.; Xie, D.; Liang, Y.; Wang, J. How to govern the big data discriminatory pricing behavior in the platform service supply chain? An examination with a three-party evolutionary game model. *Int. J. Prod. Econ.* **2021**, *231*, 107910. [CrossRef]
17. Kuo, Y.H.; Kusiak, A. From data to big data in production research: The past and future trends. *Int. J. Prod. Res.* **2019**, *57*, 4828–4853. [CrossRef]
18. Latzer, M.; Hollnbuchner, K.; Just, N.; Saurwein, F. Chapter 19: The economics of algorithmic selection on the Internet. In *Handbook on the Economics of the Internet*; Edward Elgar Publishing: Cheltenham, UK, 2016. [CrossRef]
19. Zhou, D.; Zhang, H.; Li, Q.; Ma, J.; Xu, X. COutfitGAN: Learning to Synthesize Compatible Outfits Supervised by Silhouette Masks and Fashion Styles. *IEEE Trans. Multimed.* **2022**, *Early Access*. [CrossRef]
20. Armstrong, M. Competition in two-sided markets. *RAND J. Econ.* **2006**, *37*, 668–691. [CrossRef]
21. Calvano, E.; Calzolari, G.; Denicolo, V.; Pastorello, S. Artificial intelligence, algorithmic pricing, and collusion. *Am. Econ. Rev.* **2020**, *110*, 3267–3297. [CrossRef]
22. Gilbert, R.J. Separation: A Cure for Abuse of Platform Dominance? *Inf. Econ. Policy* **2021**, *54*, 100876. [CrossRef]
23. Choi, J.P.; Jeon, D.S.; Kim, B.C. Privacy and personal data collection with information externalities. *J. Public Econ.* **2019**, *173*, 113–124. [CrossRef]
24. van Hoboken, J.; Fathaigh, R. Smartphone platforms as privacy regulators. *Comput. Law Secur. Rev.* **2021**, *41*, 105557. [CrossRef]
25. Arrieta-Ibarra, I.; Goff, L.; Jiménez-Hernández, D.; Lanier, J.; Weyl, E.G. Should we treat data as labor? Moving beyond "free". *AEA Pap. Proc.* **2018**, *108*, 38–42. [CrossRef]
26. Bloch, F.; Demange, G. Taxation and privacy protection on Internet platforms. *J. Public Econ. Theory* **2018**, *20*, 52–66. [CrossRef]
27. Bourreau, M.; Kraemer, J.; Hofmann, J. Prominence-for-data schemes in digital platform ecosystems: Implications for platform bias and consumer data collection. In *Innovation Through Information Systems*; Ahlemann, F., Schütte, R., Stieglitz, S., Eds.; Springer: Cham, Switzerland, 2021; Volume 48, pp. 512–516.
28. Yuan, S.; Pi, D.; Zhao, X.; Xu, M. Differential privacy trajectory data protection scheme based on R-tree. *Expert Syst. Appl.* **2021**, *182*, 115215. [CrossRef]
29. Koppu, S.; SOMAYAJI, S.R.K.; Meenakshisundaram, I.; Wang, W.; Su, C. Fusion of Blockchain, IoT and Artificial Intelligence—A Survey. *IEICE Trans. Inf. Syst.* **2022**, *105*, 300–308. [CrossRef]
30. Wang, W.; Yang, Y.; Yin, Z.; Dev, K.; Zhou, X.; Li, X.; Qureshi, N.M.F.; Su, C. BSIF: Blockchain-based secure, interactive, and fair mobile crowdsensing. *IEEE J. Sel. Areas Commun.* **2022**, *40*, 3452–3469. [CrossRef]

31. Wang, W.; Chen, Q.; Yin, Z.; Srivastava, G.; Gadekallu, T.R.; Alsolami, F.; Su, C. Blockchain and PUF-based lightweight authentication protocol for wireless medical sensor networks. *IEEE Internet Things J.* **2021**, *9*, 8883–8891. [CrossRef]
32. Yang, Y.; Wei, X.; Xu, R.; Wang, W.; Peng, L.; Wang, Y. Jointly beam stealing attackers detection and localization without training: an image processing viewpoint. *Front. Comput. Sci.* **2023**, *17*, 173704. [CrossRef]
33. Grewal, R.; Chakravarty, A.; Saini, A. Governance mechanisms in business-to-business electronic markets. *J. Mark.* **2010**, *74*, 45–62. [CrossRef]
34. Shi, T.; Xiao, H.; Han, F.; Chen, L.; Shi, J. A Regulatory Game Analysis of Smart Aging Platforms Considering Privacy Protection. *Int. J. Environ. Res. Public Health* **2022**, *19*, 5778. [CrossRef]
35. Steppe, R. Online price discrimination and personal data: A General Data Protection Regulation perspective. *Comput. Law Secur. Rev.* **2017**, *33*, 768–785. [CrossRef]
36. Tanimoto, J. *Fundamentals of Evolutionary Game Theory and Its Applications*; Springer: Berlin/Heidelberg, Germany, 2015.
37. da Silva Rocha, A.B.; Salomão, G.M. Environmental policy regulation and corporate compliance in evolutionary game models with well-mixed and structured populations. *Eur. J. Oper. Res.* **2019**, *279*, 486–501. [CrossRef]
38. Ji, S.f.; Zhao, D.; Luo, R.j. Evolutionary game analysis on local governments and manufacturers' behavioral strategies: Impact of phasing out subsidies for new energy vehicles. *Energy* **2019**, *189*, 116064. [CrossRef]
39. Bao, A.R.H.; Liu, Y.; Dong, J.; Chen, Z.P.; Chen, Z.J.; Wu, C. Evolutionary Game Analysis of Co-Opetition Strategy in Energy Big Data Ecosystem under Government Intervention. *Energies* **2022**, *15*, 2066. [CrossRef]
40. Encarnação, S.; Santos, F.P.; Santos, F.C.; Blass, V.; Pacheco, J.M.; Portugali, J. Paths to the adoption of electric vehicles: An evolutionary game theoretical approach. *Transp. Res. Part Methodol.* **2018**, *113*, 24–33. [CrossRef]
41. Yang, Z.; Shi, Y.; Li, Y. Analysis of intellectual property cooperation behavior and its simulation under two types of scenarios using evolutionary game theory. *Comput. Ind. Eng.* **2018**, *125*, 739–750. [CrossRef]
42. Cai, G.; Kock, N. An evolutionary game theoretic perspective on e-collaboration: The collaboration effort and media relativeness. *Eur. J. Oper. Res.* **2009**, *194*, 821–833. [CrossRef]
43. Yu, H.; Zeng, A.Z.; Zhao, L. Analyzing the evolutionary stability of the vendor-managed inventory supply chains. *Comput. Ind. Eng.* **2009**, *56*, 274–282. [CrossRef]
44. Mahmoudi, R.; Rasti-Barzoki, M. Sustainable supply chains under government intervention with a real-world case study: An evolutionary game theoretic approach. *Comput. Ind. Eng.* **2018**, *116*, 130–143. [CrossRef]
45. Li, B.; Wang, Q.; Chen, B.; Sun, T.; Wang, Z.; Cheng, Y. Tripartite evolutionary game analysis of governance mechanism in Chinese WEEE recycling industry. *Comput. Ind. Eng.* **2022**, *167*, 108045. [CrossRef]
46. Mirzaee, H.; Samarghandi, H.; Willoughby, K. A three-player game theory model for carbon cap-and-trade mechanism with stochastic parameters. *Comput. Ind. Eng.* **2022**, *169*, 108285. .: 10.1016/j.cie.2022.108285. [CrossRef]
47. Friedman, D. On economic applications of evolutionary game theory. *J. Evol. Econ.* **1998**, *8*, 15–43. [CrossRef]
48. Wen-jun, J. Will Data Advantages Increse Platform Companies' Pricing?—Model Derivation and Theoretical Analysis. *Chin. J. Manag. Sci.* **2021**, *29*, 227–237. [CrossRef]
49. Pellefigue, J. The French Digital Service Tax An Economic Impact Assessment. *Deloitte Taj* **2019**, *22*, 1–4.
50. Cyberspace Administration of China, n. The Person in Charge of the State Internet Information Office on the Drops of the Global Shares Limited by Law to Make Network Security Review-Related Administrative Punishment Decision to Answer Reporters' Questions. 2022. Available online: http://www.cac.gov.cn/2022-07/21/c_1660021534364976.htm (accessed on 22 September 2022).
51. BBC News, n. Facebook Fined €17 m for Breaching EU Data Privacy Laws. 2022. Available online: https://www.bbc.com/news/articles/cp9yenpgjwzo (accessed on 22 September 2022).
52. NBC News. TikTok is Violating Children's Privacy. 2020. Available online https://www.nbcnews.com/tech/security/tiktok-violating-children-s-privacy-advocacy-groups-warn-n1207716 (accessed on 22 September 2022).
53. Micheli, M.; Ponti, M.; Craglia, M.; Berti Suman, A. Emerging models of data governance in the age of datafication. *Big Data Soc.* **2020**, *7*, 2053951720948087. [CrossRef]
54. Aridor, G.; Che, Y.K.; Salz, T. The Effect of Privacy Regulation on the Data Industry: Empirical Evidence from GDPR. In Proceedings of the 22nd ACM Conference on Economics and Computation, Phoenix, AZ, USA, 24–28 June 2019; pp. 93–94.
55. Mikalef, P.; Lemmer, K.; Schaefer, C.; Ylinen, M.; Fjørtoft, S.O.; Torvatn, H.Y.; Gupta, M.; Niehaves, B. Examining how AI capabilities can foster organizational performance in public organizations. *Gov. Inf. Q.* **2023**, *40*, 101797. [CrossRef]