symmetry

MDPI

Article

Personal Data Value Realization and Symmetry Enhancement Under Social Service Orientation: A Tripartite Evolutionary Game Approach

Dandan Wang * and Junhao Yu

School of Business, Henan University of Science and Technology, Luoyang 471023, China; 230320291684@stu.haust.edu.cn
* Correspondence: wangdandan@haust.edu.cn

Abstract

In the digital economy, information asymmetry among individuals, data users, and governments limits the full realization of personal data value. To address this, "symmetry enhancement" strategies aim to reduce information gaps, enabling more balanced decision-making and facilitating efficient data flow. This study establishes a tripartite evolutionary game model based on personal data collection and development, conducts simulations using MATLAB R2024a, and proposes countermeasures based on equilibrium analysis and simulation results. The results highlight that individual participation is pivotal, influenced by perceived benefits, management costs, and privacy risks. Meanwhile, data users' compliance hinges on economic incentives and regulatory burdens, with excessive costs potentially discouraging adherence. Governments must carefully weigh social benefits against regulatory expenditures. Based on these findings, this paper proposes the following recommendations: use personal data application scenarios as a guide, rely on the construction of personal trustworthy data spaces, explore and improve personal data revenue distribution mechanisms, strengthen the management of data users, and promote the maximization of personal data value through multi-party collaborative ecological incentives.

Keywords: personal data; value realization; stakeholders; evolutionary game

check for updates

Academic Editor: Jie Yang

Received: 31 May 2025
Revised: 27 June 2025
Accepted: 3 July 2025
Published: 5 July 2025

Citation: Wang, D.; Yu, J. Personal Data Value Realization and Symmetry Enhancement Under Social Service Orientation: A Tripartite Evolutionary Game Approach. *Symmetry* **2025**, *17*, 1069. https://doi.org/10.3390/sym17071069

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

With the vigorous development of emerging digital technologies such as the Internet and cloud computing, data have become an important factor of production in modern society. Personal data means any information relating to an identified or identifiable natural person (data subject) [1], usually including names, phone numbers, ID card numbers, consumption records, location information, and so on. Because this information is closely related to individual identity, it has a significant need for privacy protection. Compared with corporate data, personal data have advantages in terms of subject relevance, verifiability, and reusability. They can achieve efficient circulation and utilization across different scenarios. By associating with identity identifiers, personal data can form a comprehensive individual information profile, thereby significantly improving the accuracy of service decision-making [2]. The circulation and use of personal data help achieve social sustainability by promoting public service optimization and spurring social innovation and progress.

Balancing the maximization of personal data value with the protection of its security has become a shared global goal. The UK's Midata platform aggregates consumer data

for individual use, empowering people to gain a comprehensive understanding of their consumption behaviors and control access to their data by enterprises and institutions [3]. South Korea's MyData model, initially launched in the financial sector, has gradually expanded into healthcare, transportation, and other industries [4]. Although China has made considerable efforts in developing and utilizing personal data, its actual circulation rate remains low. The primary reasons are information asymmetry and value perception asymmetry. This information asymmetry makes it difficult for data subjects to truly control the value of their own data [5–7]. They cannot accurately assess the risks associated with the use of their data, nor can they reasonably demand corresponding value in return. This value perception asymmetry leads to conflicts in the data valorization process [8,9]. Data users may excessively exploit the commercial value of data, while data subjects may resist reasonable data utilization due to privacy concerns. This asymmetry has made the relationships among data subjects, data users, and government regulators both complex and delicate, giving rise to a series of data-governance challenges—such as low data circulation rates and difficulties in balancing data value—that urgently require thorough investigation and resolution.

Currently, the academic community has conducted research on the value realization of personal data from multiple perspectives, such as data trusts, revenue distribution, and ownership allocation. However, there is a scarcity of literature that delves into the decision-making behaviors of the main stakeholders in the process of personal data value realization. In light of this, this paper attempts to utilize the theory of evolutionary game to construct a dynamic game model involving the following three parties: individuals, data users, and the government. Based on an analysis of the process of personal data collection and development and utilization, this paper systematically examines the strategy choices of each entity in the process of personal data value realization. It also explores ways to alleviate the obstacles to symmetry in the process of personal data value realization. This research aims to provide a reference for building a localized and sustainable model for personal data management and utilization in China, in order to promote high-quality social services and the continuous prosperity of the digital economy. Therefore, the focus of this study is to explore strategies that alleviate information and value asymmetries among stakeholders and accelerate the circulation of personal data value.

2. Literature Review

2.1. Personal Data Valuation

The market-oriented allocation process of personal data elements is accelerating. How to promote the efficient circulation and application of personal data to maximize their value has become a focal point for both the academic community and policy makers. Scholars have conducted research on the connotation, pathways, and influencing factors of personal data value realization.

In terms of the connotation of personal data value realization, scholars have argued and emphasized the significant economic and social value of personal data. Sun et al. showed through large-scale experiments that turning off e-commerce platforms' personalized recommendation features can cause an 81.1% drop in transaction volume, highlighting personal data's central role in platform economies [10]. Shen et al. argued that personal data have huge commercial value and proposed a personal data pricing model based on parameters like information entropy, weights, data reference indices, and costs to measure the value of big personal data [11]. Based on Nancy Fraser's "abnormal justice" theory, Cinnamon et al. analyzed the unequal positions of individuals and companies in personal data accumulation and said personal data have social value in promoting a more democratic society [12].

In terms of the pathways of personal data value realization, Janeček conducted an in-depth analysis of the entire process of personal data value realization. They comprehensively expounded the mechanisms for the realization of personal data value from three dimensions, which were theory, technology, and institutional logic [13]. Vandercruysse, from the perspective of personal data protection, argued that personal data have both personal and public attributes. He suggested that expanding the public nature of personal data can achieve greater social value [14]. Radosevic believed that personal data trusts can enhance the quality and reliability of data information and help to better realize value during the collection, processing, and application of data by data controllers [15]. Asgarinia argued that the data trust model can help address the imbalance of rights between data controllers and data subjects, promote the realization of informed consent in personal data use, and enhance trust between data subjects and data platforms [16].

In terms of the factors affecting the realization of personal data value, scholars have conducted research from aspects such as data ownership, data governance, privacy technologies, and public attitudes. Burri analyzed the constraining role of exclusive property rights on the realization of personal data value and proposed exploring a permissive personal data usage scheme [17]. Park et al. argued that the construction of a trustworthy data space is key to empowering the real economy with the digital economy. However, this cannot rely solely on technological support. It is necessary to build a commercial data element ecosystem to explore the large-scale application of personal data [18]. Pena et al. pointed out that the public's concerns about data security and financial privacy breaches have become a key barrier to bank data sharing. These concerns have significantly weakened industry trust and constrained business expansion [19]. In summary, scholars have conducted in-depth research on the value realization of personal data from multiple dimensions, covering the connotation and pathways and influencing factors of personal data value realization, providing rich references for related research and practice.

2.2. Application of Evolutionary Game Theory

Evolutionary game theory, based on the assumption of bounded rationality among participants, is commonly used to study the mutual influence of strategic choices among different actors. As a branch of game theory, it introduces concepts from biological evolution into game-theoretic analysis. It primarily focuses on how individual (or group) strategies evolve over time in response to environmental changes and interactions. This theory has been widely applied in fields such as sociology and economics. In the specific domain of data circulation and utilization, scholars have conducted research on issues such as privacy disclosure, data governance, and value distribution.

With the rise of internet platforms, situations where users exchange personal data for free services have become increasingly common, attracting the attention of researchers. Scholars have explored the impact of privacy concerns on privacy disclosure. For example, Xu et al. argued that, in online health communities, users' privacy disclosure behaviors are influenced not only by their own privacy awareness but also by external factors (such as community rewards and privacy protection policies) [20]. Majeed et al. proposed using methods like random forests and the Simpson index to assess the level of data privacy and to quantify privacy risks during the anonymization of personally identifiable information (PII) [21]. Wang et al. analyzed the strategic choices of information entities and information operators from the perspective of personal information protection [22]. Dimodugno et al. examined whether individuals would agree to share their data at different levels of data sensitivity from the perspective of personal data consent mechanisms [23]. Wan used a Stackelberg game model to analyze the impact of external attacks on large-scale genomic data sharing [24].

With the deepening application of evolutionary game theory in data governance research, scholars have started to explore the regulatory mechanisms and guiding role of governments. For instance, Zhu et al. proposed that, in response to the passive rights protection issues faced by APP users, the government should improve incentive-based regulatory measures that balance incentives and constraints, aiming to maximize the effectiveness of personal information security supervision for apps [25]. Zhang pointed out the regulatory challenges in the digital market, emphasizing that the government should play a leading role by establishing legal frameworks for data privacy and security. This would protect end-user rights while not hindering innovation, thereby addressing issues of unfair competition in the digital market [26].

Data circulation is expected to generate tremendous value, and scholars have conducted research on how to assess and distribute this value. For example, Cheong et al. adopted a cost-based approach and applied differentiated valuation strategies based on the characteristics of different types of data assets held by enterprises, effectively reducing repetition in the evaluation process and improving accuracy and applicability [27]. Li et al. proposed a blockchain-based multidimensional collaboration framework, which utilizes a multi-attribute value assessment method to help enterprise collaborators reach a consensus on shared data, providing a more comprehensive evaluation framework for data circulation [28]. Lrina introduced a game-theory-based fair revenue model using the Shapley value allocation principle to estimate the value generated by data providers, encouraging cooperation and competition among data enterprises [29]. Zhu et al. used evolutionary game theory to balance fairness and efficiency by adjusting privacy sensitivity parameters and profit distribution coefficients, proposing a profit distribution strategy between individuals and enterprises [8].

Scholars have deeply explored personal data governance in terms of the connotation, path, and influential factors of personal data value realization, laying a theoretical foundation for this paper. The wide application of evolutionary game theory studying in various aspects of personal data value has also been verified to be suitable for this paper.

3. Model Construction

3.1. Problem Description

In Korea's MyData model, personal data operators create authorization platforms offering efficient management tools. Users first log in to an application system developed by the operator to exercise their right to data portability. The operator then uses encrypted API connections to securely and efficiently consolidate personal data that is dispersed among various data controllers—such as medical and financial institutions. Users can easily access basic data services through the platform and independently view and manage their data, enhancing inquiry efficiency and service experience while enjoying value-added services [30]. Data application organizations, like banks and insurance companies, obtain data through APIs and provide users with personalized services such as credit, asset, and health management by combining precise analysis. These organizations acquire the required data resources to conduct related services and pay data controllers and operators based on API calls. This payment model ensures that data controllers provide data resources and compensate operators for their data integration and service efforts, guaranteeing the sustainable realization of personal data value. Korea's MyData model adopts an opt-out mechanism, safeguarding users' autonomy over data usage [31]. Personal data operators must undergo strict government review and meet certain conditions to qualify. As a core link in the data industry chain, operators collect scattered information to offer users one-stop services. For instance, banks and other financial institutions can use user-authorized data to provide individuals with higher loan limits or lower-interest loans if they have good

credit ratings. This benefits users and helps banks expand their customer base and increase market share. This mutually empowering model not only improves the user experience but also creates stronger market competitiveness and profitability for data application organizations, fully realizing the social benefits of personal data. The flowchart of personal data collection and utilization is as shown in Figure 1.

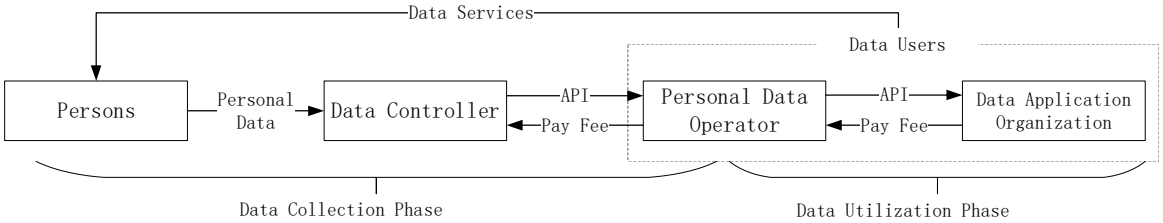


Figure 1. Flowchart of personal data collection and utilization.

However, in real-world scenarios, there is a significant difference in the perception of data value between data subjects and data users. For data subjects, they may focus more on the privacy value of data and hope that their data will not be leaked or misused. For example, users may believe that the health data they enter in a medical and health application are valuable mainly for protecting personal privacy and health safety. In contrast, data users place greater emphasis on the commercial value of data, such as analyzing this health data to develop new medical products or formulate insurance strategies. Data users may overlook the privacy value concerns of data subjects in pursuit of commercial benefits. In addition, the government faces difficulties in supervision, as well as insufficient regulatory guidance and safeguard measures for data circulation. We believe that individuals have complex considerations when deciding whether to participate in personal data sharing. Their decision to participate is influenced by factors such as the data services they obtain through participation, the privacy invasion risks associated with personal data sharing, and the development of the government's privacy and security environment. Therefore, the focus of this study is on how to mitigate information asymmetry, trust asymmetry, and behavioral asymmetry among stakeholders and how to accelerate the flow of personal data value.

3.2. Model Assumptions

The game-like relationships among individuals, data users, and the government are shown in Figure 2. Meanwhile, the game tree is used to illustrate the specific process of the game and consists of nodes and branches. The nodes represent the decision points of the participants, with a total of seven decision points in this game. The endpoints of the game tree represent the various strategy combinations. The game tree involving the individual, data users, and the government is shown in Figure 3.

Individuals, as data owners, decide whether to participate in personal data aggregation. If they participate, then they can use basic services like data integration and inquiry, as well as value-added services such as personalized loan recommendations and credit-score improvement initiatives. However, this comes with privacy-breach-related risks. Non-participation means no involvement in personal data development and utilization. Thus, individuals can choose between "participate" and "not participate".

Data users decide on compliant or non-compliant data usage. Compliant usage requires investment in data-service development and necessary data-security technology to guarantee legality and safety. Conversely, non-compliant operation means minimal investment in data-security technology and excessive data usage for more potential gains. Thus, personal data operators can choose between "compliant use" and "non-compliant use".

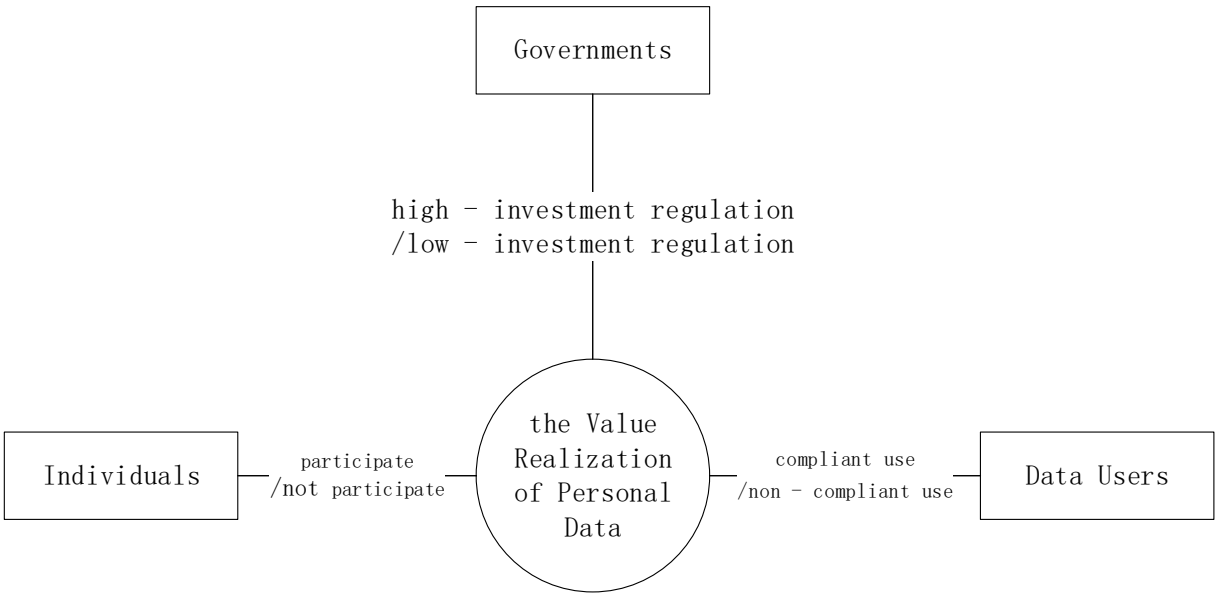


Figure 2. Evolutionary game model of individuals, data users, and governments.

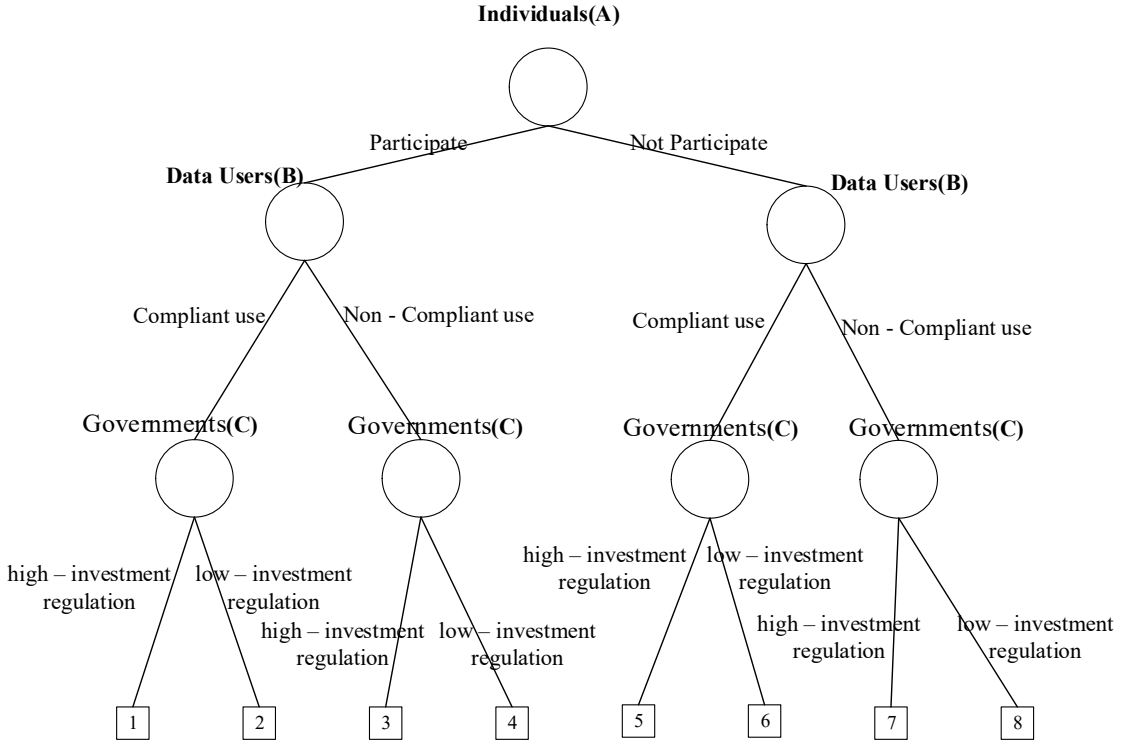


Figure 3. Tripartite game diagram of individuals, data users, and governments. The numbers 1–8 represent all the combinations of behavioral strategies.

The government is responsible for overseeing data users' actions to guarantee data-usage compliance and safety. When choosing high-investment regulation, it increases the budget for stricter compliance checks on data users. Total regulatory cost covers spending on technology enhancement, personnel, equipment, etc. Conversely, low-investment regulation means laxer oversight and reduced regulatory spending. Thus, the government can choose between "high-investment regulation" and "low-investment regulation".

Assumption 1. *Individuals, data users, and the government are all bounded rational agents, each holding different expectations regarding the short-term and long-term benefits of participation. In the early stages, both individuals and data users primarily focus on short-term benefits, while the*

government places more emphasis on long-term gains. In the short term, all three parties in the game make decisions based on the goal of maximizing their own benefits, and their behavior choices exhibit characteristics of probability distribution. However, in the long term, the three parties will gradually establish a stable cooperative relationship through coordination and collaboration, actively circulating and utilizing personal data to achieve greater social and economic benefits.

Assumption 2. *Let x represent the proportion of individuals choosing to participate, and $1-x$ represent the proportion choosing not to participate, $x \in [0,1]$. Let y represent the proportion of data users opting for compliant data usage, and $1-y$ the proportion opting for non-compliant usage, $y \in [0,1]$. Let z represent the proportion of governments selecting high-investment regulation, and $1-z$ the proportion selecting low-investment regulation, $z \in [0,1]$.*

Assumption 3. *This assumption regards the benefits and costs for individuals. When an individual participates, the total benefit they can obtain is R_1, which includes the benefits from basic data services such as data inquiry and data invocation, as well as the benefits from value-added services such as personalized recommendations and financial services. After participating, individuals need to spend time and effort on data management, denoted as C_1. They also bear certain risks of data leakage and abuse, which are L. When data users use data compliantly, the probability of an individual suffering losses is a; when data users use data non-compliantly, the probability is b. When personal data operators use data compliantly, they can somewhat lower data-leakage and abuse risks. Hence, $a < b$.*

Assumption 4. *This assumption regards data users' benefits and costs. If an individual participates, then the data user's total benefit is R_2, covering economic and social aspects. To uphold its image, the data user will incur total costs of C_2, which include compliance and operational costs. Compliance costs relate to expenses on equipment, technology, personnel, etc., while operational costs involve data invocation fees, etc., all aimed at supporting personal data circulation and usage. The total cost for compliant usage is C_3; for non-compliant usage, it is f. As non-compliant data usage involves relatively lower safety and operational costs, $C_2 > C_3$. Although non-compliant usage can generate extra benefits of R_3, it also faces government regulatory risks. Under high-investment regulation, the probability of being caught for non-compliant use is k_1, with a fine of F; under low-investment regulation, the probability of being caught is k_2.*

Assumption 5. *This assumption regards the benefits and costs for the government. As the leading entity in personal data development and utilization, the government bears the responsibility of constructing an open, efficient, and secure environment for personal data utilization. It is in charge of building a safety framework for personal data value realization and monitoring the compliance of all data users. Therefore, it must invest in regulatory costs. When the government selects a high-investment regulatory model, the regulatory cost is g_1, it yields social benefits of R_4, and the probability of detecting non-compliant data usage by enterprises is k_1. Under a low-investment regulatory model, the regulatory cost is g_2, it yields social benefits of R_5, and the detection probability is k_2. In the high-investment regulatory model, the government invests more in regulation and is more likely to detect non-compliant behavior by data users; thus, $g_1 > g_2$, $k_1 > k_2$. The government imposes a penalty of F for non-compliant data usage by enterprises. The variables and parameters related to the above model are presented in Appendix A.*

3.3. Payoff Matrix

Based on the above basic assumptions, when the individual providing data chooses to "participate", the data user chooses "compliant use", and the government chooses the "high investment in regulation" strategy, the individual's payoff is the sum of the trust benefit from the individual (T) and the basic benefit obtained from providing personal data (R_1), minus the cost of managing the data (C_1) and the privacy risk loss ($a * L$). Similarly,

the payoff formulas for the individual, data user, and government can be derived, as shown in Table 1.

Table 1. The revenue matrices of the game stakeholders under each strategy combination.

Individuals	Data Users	Governments	
		High-Regulation	**Low-Regulation**
Participation	compliance	$T + R_1 - C_1 + a * L$, $R_2 - C_2$, $R_4 - g_1$	$T + R_1 - C_1 + b * L$, $R_2 - C_2$, $R_5 - g_2$
	Non-compliance	$R_1 - C_1 + a * L$, $R_2 + R_3 - C_3 - k_1 * F$, $R_4 - g_1 + k_1 * F$	$R_1 - C_1 + b * L$, $R_2 + R_3 - C_3 - k_2 * F$, $R_5 - g_2 + k_2 * F$
Non-Participation	compliance	0, $-C_2$, $-g_1$	0, $-C_2$, $-g_2$
	Non-compliance	0, $-C_3$, $-g_1$	0, $-C_3$, $-g_2$

4. Evolutionary Game Equilibrium Analysis

4.1. Expected Payoff Function Construction

Based on the payoff matrix of the game players in Table 2, the expected payoff function of individuals can be constructed as follows:

Table 2. Stability analysis of equilibrium points in tripartite evolutionary games.

Equilibrium Point	Eigenvalues λ_1	Eigenvalues λ_2	Eigenvalues λ_3	Stability Analysis
$E_1(0,0,0)$	$R_1 - C_1 - L * b$	$C_3 - C_2 < 0$	$g_2 - g_1 < 0$	Saddle OR ESS
$E_2(1,0,0)$	$C_1 - R_1 + L * b$	$C_3 - C_2 - R_3 + F * k_2$	$g_2 - g_1 + R_4 - R_5 + F * (k_1 - k_2)$	Saddle OR ESS
$E_3(0,1,0)$	$R_1 + T - C_1 - L * b$	$C_2 - C_3 > 0$	$g_2 - g_1 < 0$	unstable
$E_4(0,0,1)$	$R_1 - C_1 - L * a$	$C_3 - C_2 < 0$	$g_1 - g_2 > 0$	unstable
$E_5(1,1,0)$	$C_1 - T - R_1 + L * b$	$C_2 - C_3 + R_3 - F * k_2$	$g_2 - g_1 + R_4 - R_5$	Saddle OR ESS
$E_6(0,1,1)$	$T - C_1 + R_1 - L * a$	$C_2 - C_3 > 0$	$g_1 - g_2 > 0$	unstable
$E_7(1,0,1)$	$C_1 - R_1 + L * a$	$C_3 - C_2 - R_3 + F * k_1$	$g_1 - g_2 + R_5 - R_4 - F * k_1 + F * k_2$	Saddle OR ESS
$E_8(1,1,1)$	$C_1 - T - R_1 + L * a$	$C_2 - C_3 + R_3 - F * k_1$	$g_1 - g_2 - R_4 + R_5$	Saddle OR ESS

The expected payoff when individuals choose to participate is U_{11}, and that when they opt out is U_{12}. The average expected payoff of individuals is U_1, and the equations used to obtain them are shown as follows:

$$U_{11} = y * z * (R_1 - C_1 - a * L + T) + (1 - y) * z * (R_1 - C_1 - a * L) + y * (1 - z) * (R_1 - C_1 - b * L + T) + (1 - y) * (1 - z) * (R_1 - b * L - C_1) \quad (1)$$

$$U_{12} = 0 \quad (2)$$

$$U_1 = x * U_{11} + (1 - x) * U_{12} = -x * (C_1 - R_1 + L * b - T * y + L * a * z - L * b * z) \quad (3)$$

Similarly, according to the calculation formula of the replicator dynamic equation, the replicator dynamic equations for individuals, data users, and the government are obtained as follows:

$$f(x) = x(U_{11} - U_1) = x * (x - 1) * (C_1 - R_1 + L * b - T * y + L * a * z - L * b * z) \quad (4)$$

$$f(y) = y(U_{21} - U_2) = y * (y-1) * (C_3 - C_4 + R_3 * x - F * k_2 * x - F * k_1 * x * z + F * k_2 * x * z) \quad (5)$$

$$f(z) = z(U_{31} - U_3) = z * (z-1) * (g_1 - g_2 - R_4 * x + R_5 * x - F * k_1 * x + F * k_2 * x + F * k_1 * x * y - F * k_2 * x * y) \quad (6)$$

4.2. Stability Analysis

The strategy choices of individuals, data users, and the government are dynamic. When their replicator dynamic equations equal zero, the game is stable. Setting $f(x) = f(y) = f(z) = 0$ yields the following nine potential equilibrium points: [$E_1(0,0,0)$, $E_2(1,0,0)$, $E_3(0,1,0)$, $E_4(0,0,0)$, $E_5(1,1,0)$, $E_6(0,1,1)$, $E_7(1,0,1)$, $E_8(1,1,1)$, $E_9(x^*, y^*, z^*)$]. As stable points in evolutionary games must be strict Nash equilibria, only eight pure strategy solutions are discussed.

Per evolutionary game stability theory, the Jacobian matrix studies the stability of local equilibrium points in strategy space [32]. If all eigenvalues of the Jacobian matrix J, constructed as follows, have negative real parts at a potential equilibrium point, then that point is asymptotically stable:

$$J = \begin{bmatrix} \frac{f(x)}{\partial x} & \frac{f(x)}{\partial y} & \frac{f(x)}{\partial z} \\ \frac{f(y)}{\partial x} & \frac{f(y)}{\partial y} & \frac{f(y)}{\partial z} \\ \frac{f(z)}{\partial x} & \frac{f(z)}{\partial y} & \frac{f(z)}{\partial z} \end{bmatrix} = \begin{bmatrix} f_{11} & f_{12} & f_{13} \\ f_{21} & f_{22} & f_{23} \\ f_{31} & f_{32} & f_{33} \end{bmatrix} \quad (7)$$

where

$$f_{11} = (2x-1) * (C_1 - R_1 + L * b - T * y + L * a * z - L * b * z)$$
$$f_{12} = -T * x * (x-1)$$
$$f_{13} = x * (L * a - L * b) * (x-1)$$
$$f_{21} = y * (y-1) * (R_3 - F * k_2 - F * k_1 * z + F * k_2 * z)$$
$$f_{22} = (2y-1) * (C_2 - C_3 + R_3 * x - F * k_2 * x - F * k_1 * x * z + F * k_2 * x * z)$$
$$f_{23} = -y * (F * k_1 * x - F * k_2 * x) * (y-1)$$
$$f_{31} = -z * (z-1) * (R_4 - R_5 + F * k_1 - F * k_2 - F * k_1 * y + F * k_2 * y)$$
$$f_{32} = z * (F * k_1 * x - F * k_2 * x) * (z-1)$$
$$f_{33} = (2z-1) * (g_1 - g_2 - R_4 * x + R_5 * x - F * k_1 * x + F * k_2 * x + F * k_1 * x * y - F * k_2 * x * y)$$

Substituting all equilibrium points into the Jacobian matrix yields the eigenvalues in Table 2. By Lyapunov's indirect method, if all eigenvalues of the Jacobian matrix are less than 0, then the equilibrium point is asymptotically stable. If at least one eigenvalue is positive, then it is a saddle or unstable point. If eigenvalues are both 0 and negative, then stability is indeterminate. Thus, potential stable points $E_3(0,1,0)$, $E_4(0,0,1)$, and $E_6(0,1,1)$ are unstable, while the other five ($E_1(0,0,0)$, $E_2(1,0,0)$, $E_5(1,1,0)$, $E_7(1,0,1)$, and $E_8(1,1,1)$) are stable.

Local stability analysis of the five stable points based on the above conditions and assumptions is shown as follows:

Scenario 1: For $E_1(0,0,0)$ and $E_2(1,0,0)$, $E_1(0,0,0)$ is asymptotically stable when $R_1 < C_1 + L * b$, $C_3 < C_2$, and $g_2 < g_1$. Similarly, $E_2(1,0,0)$ is asymptotically stable when $C_1 + L * b < R_1$, $F*k_2 < R_3 + C_2 - C_3$, and $R_4 - R_5 + F * (k_1 - k_2) < g_1 - g_2$. If an individual's service revenue from participation is less than the sum of privacy loss and data management costs, then they will refuse to participate. This leads to a (0, 0, 0) equilibrium, reflecting the early stage of personal data value, where data infrastructure is underdeveloped and participation enthusiasm is low. Conversely, if perceived benefits exceed risks, then individuals will participate. However, the government may opt for low-intensity regulation due to high additional regulatory costs, and data users may abuse

personal data due to the high profits from data misuse, resulting in a (1, 0, 0) equilibrium. This mirrors the "privacy paradox" [33], where people agree to privacy policies despite knowing that data might be misused, turning a blind eye to potential risks.

Scenario 2: For $E_7(1,0,1)$ and $E_8(1,1,1)$, $E_7(1,0,1)$ is an asymptotically stable point when $C_1 + L * a < R_1$, $F * k_1 < R_3 + C_2 - C_3$, and $g_1 - g_2 < R_4 - R_5 + F * (k_1 - k_2)$. Similarly, $E_8(1,1,1)$ is an asymptotically stable point when $C_1 + L * a < R_1 + T$, $R_3 + C_2 - C_3 < F * k_1$, and $g_1 - g_2 < R_4 - R_5$. In this case, if the individual net profit is positive, then participation will be chosen rationally. The government will assess the long-term benefits based on the additional social welfare generated by personal data development and utilization. If the long-term benefits are high, then the government will be willing to invest extra regulatory costs in maintaining data utilization order. Data users will weigh the benefits of misusing personal data and the cost savings on security against the potential fines. If the potential fines are high, then they will choose to use personal data in compliance, forming a (1,1,1) game equilibrium. If the potential fines are low, then they will choose to misuse personal data, forming a (1,0,1) game equilibrium. This corresponds to the stage of personal data value development. The government fully recognizes the value of personal data development and continuously invests in regulatory costs while providing more convenient infrastructure and social services for individuals and strengthening the ongoing supervision of data users to ensure personal data security.

Scenario 3: For $E_5(1,1,0)$, it is an asymptotically stable point when $C_1 + L * b < T + R_1$, $R_3 + C_2 - C_3 < F * k_2$, and $R_4 - R_5 < g_1 - g_2$. Data users will opt for compliant personal data usage if their improper gains plus cost savings are less than the penalty for violations. If data users voluntarily comply, then the government, considering that additional regulatory costs do not bring extra social welfare, will adopt a low-input regulatory strategy. This leads to a (1, 1, 0) game equilibrium. Individuals participate if privacy risks are lower than participation benefits. This scenario reflects the mature stage of personal data value development. Data users recognize and exploit personal data value with high self-discipline. With robust data infrastructure and systems, the government only needs low regulatory costs to ensure proper personal data value development.

5. Simulation Analysis

To more intuitively show the dynamic process of the three-party strategy equilibrium among individuals, data users, and the government, MATLAB (R2024a) is used for numerical simulation. To pursue the ideal state of $E_8(1,1,1)$, the initial parameter values must meet the constraints of $C_1 + L * a < R_1 + T$, $C_2 - C_3 + R_3 < F * k_1$, and $g_1 - g_2 < R_4 - R_5$. The initial values are assigned as follows: $R_1 = 50$, $C_1 = 40$, $a = 0.3$, $b = 0.5$, $L = 30$, $T = 10$, $R_2 = 130$, $R_3 = 40$, $C_2 = 130$, $C_3 = 80$, $k_1 = 0.8$, $k_2 = 0.5$, $F = 150$, $R_4 = 200$, $R_5 = 150$, $g_1 = 80$, $g_2 = 50$, and $x = y = z = 0.5$. Based on this, we first investigate the mutual influence of the three parties' initial strategies. Then, we analyze the impact of key parameters like authorization management costs, service revenue, and violation fines on individual entities' behavioral strategy choices.

5.1. The Initial Willingness and Its Impact on the Strategy Evolution of the Three Parties

As an important component of a dynamic game system, the strategy choice of any one party will significantly affect the decision-making behavior of other relevant parties. Based on the initial parameter values, by gradually adjusting the initial strategies of the three parties (individuals, data users, and the government), the evolution trend of the system is observed to study the interactive effects and influences of different initial strategy combinations of the three parties on each other's evolutionary paths.

5.1.1. The Impact of Initial Willingness on the Evolution of Three Parties

As participants in the game, changes in the initial strategies of each party will influence the strategy choices of the other parties. In this paper, the initial willingness of all three parties is set to the same value (x = y = z), and three simulation runs are conducted sequentially. The evolution results are shown in Figure 3. As seen in Figure 4, when the initial willingness of all three parties is 0.2, the decisions of the three parties (x, y, z) converge to 0, and the equilibrium point tends toward (0, 0, 0). When the initial willingness of the three parties is moderate or high, the decisions of the three parties (x, y, z) all converge to 1, and the equilibrium point tends toward (1, 1, 1). Overall, as the initial willingness of all parties increases synchronously, the individual's decision (x) rapidly converges to 1, which accelerates the convergence of the decisions (y, z) of data users and the government to 1, ultimately reaching the equilibrium point (1, 1, 1).

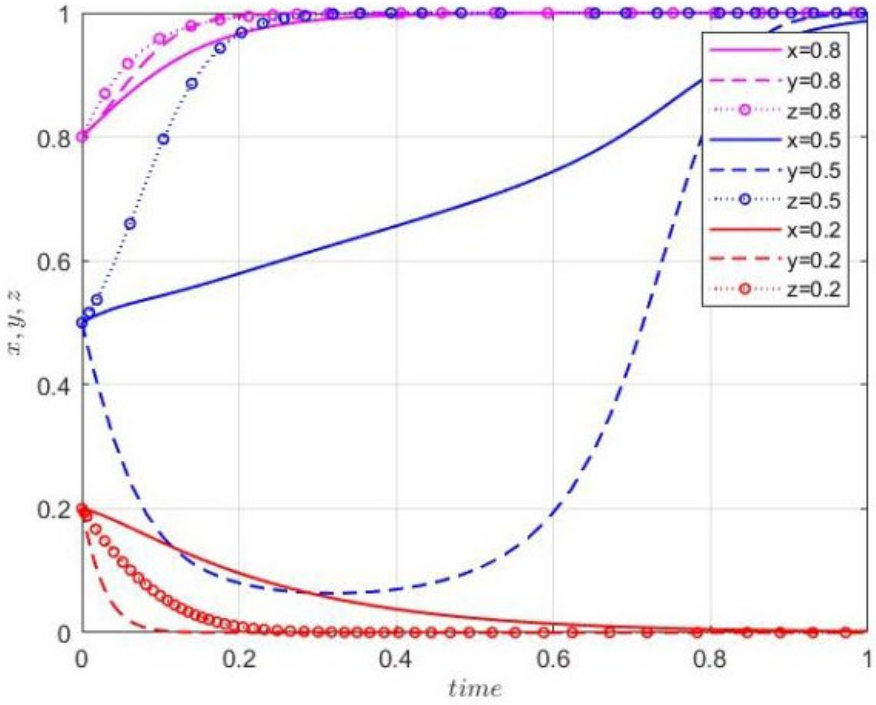
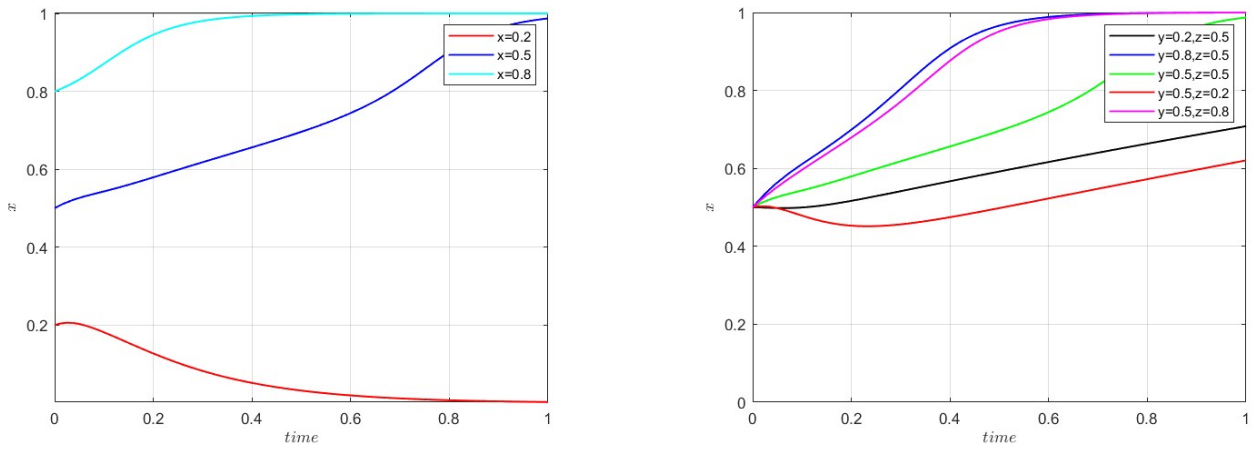


Figure 4. The evolutionary trajectory of the three parties when the initial intention changes.

5.1.2. The Impact of Initial Willingness on the Evolution of Individual Strategies

From Figure 5a, it can be seen that only when individuals have low initial willingness to participate will their strategy converge to the evolutionarily stable strategy of "non-participation". The stronger the initial willingness of individuals, the faster the evolution from "non-participation" to "participation"; that is, initial willingness exerts an accelerating effect in the evolutionary process.

As shown in Figure 5b, the evolution of individual strategies is influenced by both the initial willingness of data users and the government. The initial willingness of data users has a relatively small effect on the evolution of individual strategies, whereas that of the government has a significant impact. When the government's initial willingness is low, individuals are more likely to adopt a "non-participation" strategy initially, but over time, the strategy evolves towards "participation". On the contrary, when the government's initial willingness is high, the evolution curve of individual strategies shows an upward trend. This may be due to the fact that strict government regulation and enhanced legal compliance by data users improve the security environment for personal data circulation, thereby increasing individuals' willingness to participate and driving the strategy to evolve towards "participation".

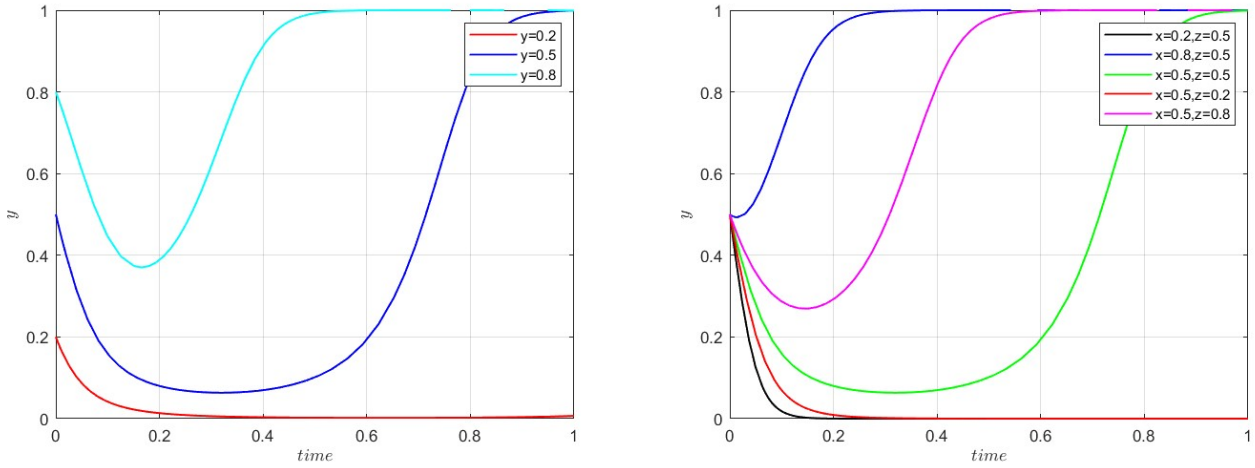


(**a**) (**b**)

Figure 5. (**a**) The evolutionary trajectory of individuals when their initial willingness changes; (**b**) the evolutionary trajectory of individuals when the initial willingness of data users and the government changes.

5.1.3. The Impact of Initial Willingness on the Evolution of Data User Strategies

From Figure 6a, it can be observed that data users only evolve towards "non-compliant use" when their initial willingness is low. This indicates that the stronger the initial willingness of data users, the more effectively it can accelerate the convergence of their strategy evolution, prompting them to more quickly converge to the evolutionarily stable strategy of "compliant use". In other words, the evolution speed of data users choosing "compliant use" gradually increases with the enhancement of initial willingness.



(**a**) (**b**)

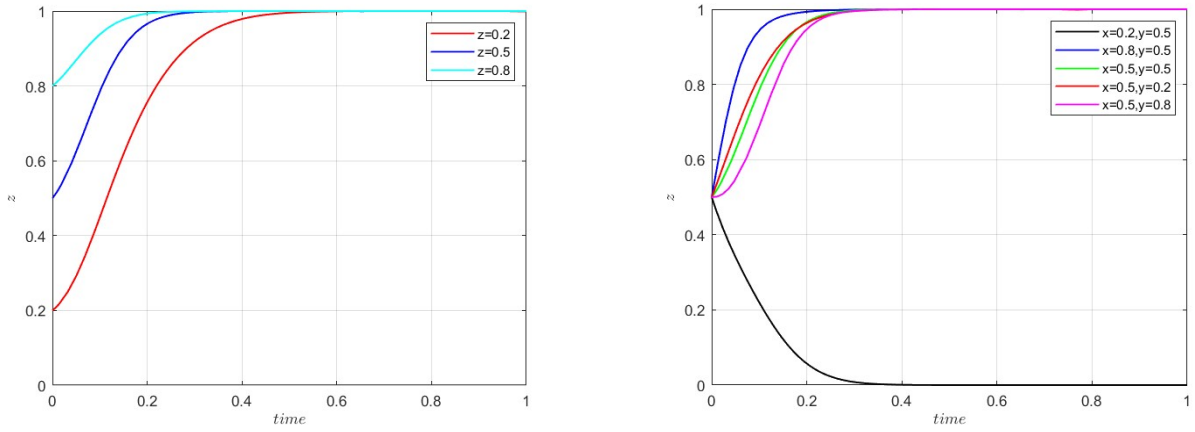
Figure 6. (**a**) The evolutionary trajectory of data users when their initial intention changes; (**b**) the evolutionary trajectory of data users when the initial intention of individuals and the government changes.

From Figure 6b, the strategy selection of data users is influenced by the initial willingness of both individuals and the government. The initial willingness of individuals has a more significant impact on the evolutionary direction of data users than that of the government. When the initial willingness of individuals is low, the rate at which data users evolve towards "non-compliant use" increases. Conversely, when the initial willingness of individuals is high, it accelerates the evolution of data users towards "compliant use". When the initial willingness of the government is high, the evolutionary curve of data users takes on an inverted "U" shape. This shows that data users initially tentatively choose

non-compliant strategies and then quickly shift to compliance, reflecting their speculative psychology and sensitivity to regulation. When the initial willingness of the government is low, data users rapidly evolve towards non-compliant strategies. This indicates that lax regulation enhances their motivation to misuse data for profit, highlighting the critical role of government regulatory intensity in the strategy selection of data users.

5.1.4. The Impact of Initial Intention on the Evolution of Government Policies

From Figure 7a, regardless of the government's initial intention, its final policy always converges to the evolutionary stable strategy of "high-input supervision". This shows that a strong initial intention of the government can significantly accelerate the policy evolution process, enabling the government to reach the high-input supervision stable state more quickly.



(**a**) (**b**)

Figure 7. (**a**) The evolutionary trajectory of the government when its initial intention changes; (**b**) the evolutionary trajectory of the government when the initial intention of individuals and data users changes.

Figure 7b shows that the evolution of government policies is influenced by the initial intentions of individuals and data users. The initial intention of individuals significantly impacts the evolution of government policies, whereas that of data users has a minimal effect. This suggests that the additional fines caused by strict government supervision play a limited role in promoting active regulation. When individuals' initial intention is low, government policies rapidly evolve towards "low-input supervision". In contrast, when individuals' initial intention is high, the evolution rate of government policies towards "high-input supervision" speeds up. This might be because active individual participation generates substantial social benefits for the government, significantly driving its shift from passive to active regulation and accelerating the policy evolution process.

In conclusion, the initial willingness of the three parties has a significant impact on their strategic choices. For individuals, the stronger their initial willingness, the faster they shift from a "non-participation" to a "participation" state. Moreover, the government's initial willingness has a notable influence on the evolution of individual strategies; when the government's initial willingness is high, the individual's strategy evolution curve shows an upward trend. For data users, the stronger their initial willingness, the faster their strategies evolve toward "compliant use". The influence of individuals' initial willingness on the evolution of data users' strategies is significantly greater than that of the government's. When individuals have low initial willingness, data users are more likely to evolve rapidly toward "non-compliant use". The government's strategies eventually converge to the evolutionarily stable strategy of "high-investment regulation". Notably, individuals' initial

willingness significantly affects the government's strategy evolution; when individuals have high initial willingness, the government's strategy evolves toward "high-investment regulation" at a faster rate.

5.2. The Impact of Data Service Revenue and Authorization Management Costs on Individuals

The simulation results in Figure 8 reveal how data service revenue (R_1) and authorization management costs (C_1) affect the evolution of individuals' "participation" strategies. When data service revenue (R_1) is fixed, rising authorization management costs (C_1) lower the adaptability of the "participation" strategy, reducing participation probability. Conversely, when authorization management costs (C_1) are fixed, increasing data service revenue (R_1) boosts the adaptability of the "participation" strategy, raising participation probability.

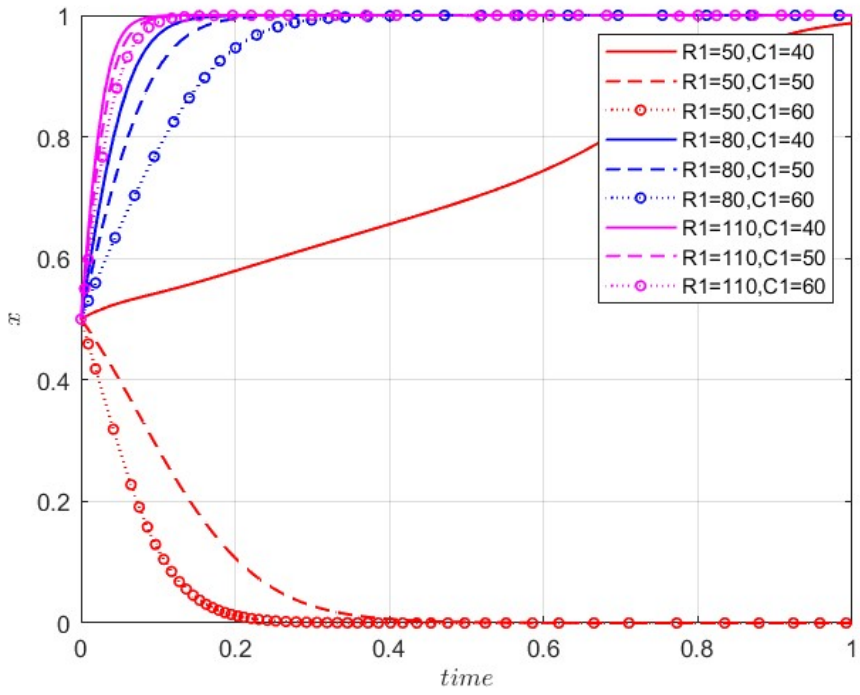


Figure 8. The evolution trajectory of individuals when the cost of authorization management and service revenue change.

From Figure 8, when data service revenue is high (R_1 = 80, R_1 = 110), the "participation" strategy always shows a stable evolutionary advantage, regardless of authorization management cost changes. But when data service revenue is low (R_1 = 50), authorization management costs become much more influential in strategy choice. Especially at high costs (C_1 = 50, C_1 = 60), participation probability drops rapidly in a nonlinear way. This shows that, in the adaptability trade-off between revenue and cost, if data service revenue cannot meet individuals' expected utility, lowering authorization management costs is key to enhancing the evolutionary stability of the "participation" strategy.

5.3. The Impact of Data Abuse Profits and Violation Penalties on Data Users

The simulation results in Figure 9 show how data abuse profits and government punishments affect data users' strategy choices regarding compliance. When data abuse profits (R_3) are fixed, the probability of compliance (y) rises as the penalty for non-compliance increases. This indicates that a strict punishment (F) mechanism significantly encourages compliance. Conversely, when penalties are fixed, the compliance probability (y) drops as data abuse profits (R_3) rise. Especially when penalties are low, if data abuse profits (R_3)

increase from 40 to 60, the user quickly evolves towards non-compliant strategies. This reflects that lenient punishments can easily lead to a mentality where users are inclined to violate rules to gain improper benefits. However, when penalties are high, even with increasing data abuse profits, the compliance curve becomes flatter, indicating users' indecision. In this case, high penalties effectively curb the impulse to choose non-compliance.

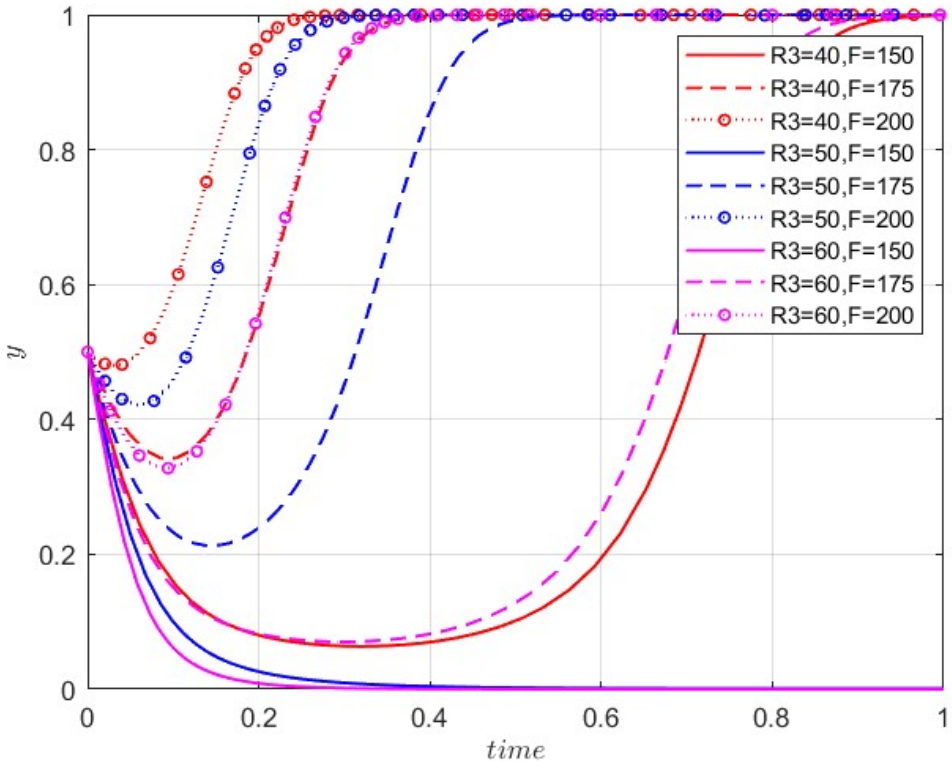


Figure 9. The evolution trajectory of data users when the benefits of data abuse and fines for violations change.

5.4. The Impact of Social Benefits and Regulatory Costs on the Government

Figure 10's simulation shows how social benefits (R_4) and regulatory costs (g_1) influence the evolution of the government's "high-input regulation" strategy. When social benefits (R_4) are constant, rising regulatory costs (g_1) make the government less likely to choose high-input regulation, showing that cost pressure can suppress regulatory enthusiasm. When regulatory costs (g_1) are fixed, higher social benefits (R_4) significantly boost the evolution of the high-input regulation strategy, making the government more inclined to adopt it. When social benefits (R_4) are low (R_4 = 200) and regulatory costs (g_1) rise from 80 to 120, the government's strategy quickly moves toward low-input regulation. In this case, social benefits cannot offset the negative effects of cost growth. When social benefits (R_4) are medium and regulatory costs (g_1) are high (g_1 = 150, g_1 = 120), the government's evolution curve fluctuates, but under ongoing cost pressure, the government will eventually choose "low-input regulation". When social benefits (R_4) are high (R_4 = 300), changes in regulatory costs (g_1) no longer affect the government's final strategy choice. The government remains stable in its high-input regulation strategy, showing path dependence. Driven by significant social benefits, the government will maintain an active regulatory stance to maximize public interest as long as regulatory costs are within the acceptable threshold.

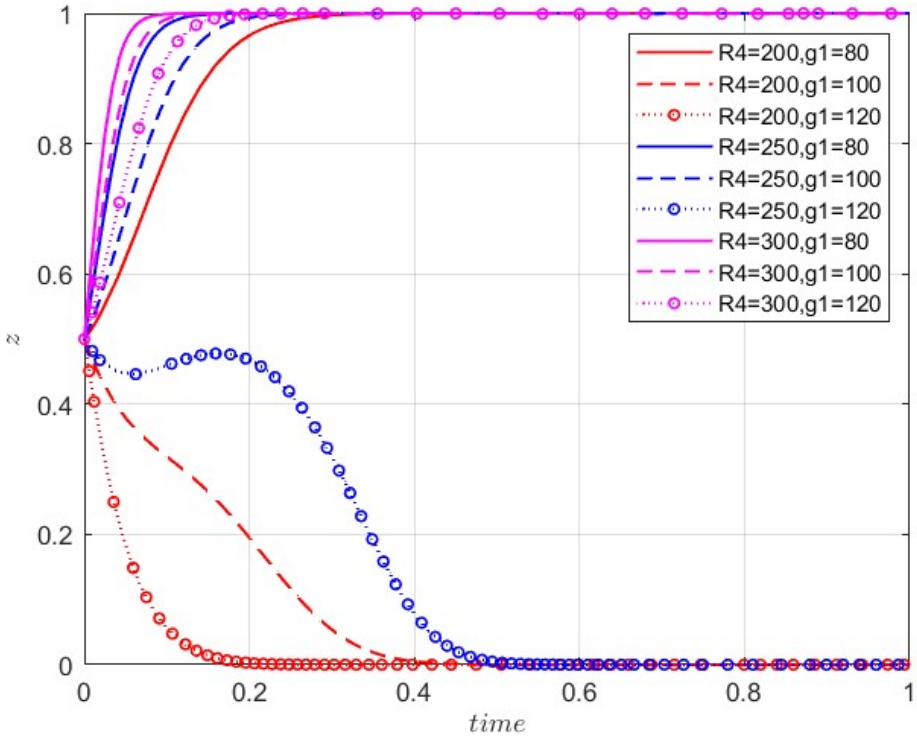


Figure 10. The evolution trajectory of the government when social benefits and regulatory costs change.

6. Conclusions

6.1. Summary and Conclusions

This study applies evolutionary game theory to explore the decision-making interactions among stakeholders in the personal data value creation process. It identifies individuals, data users, and the government as the three key players. After establishing a payoff matrix and an evolutionary game model, numerical simulations using MATLAB (R2024a) are conducted to analyze parameter impacts. The following are the key conclusions:

1. In the game process, an individual's choice to participate is the fundamental driving force behind the formation of the optimal evolutionary path. Once an individual's initial willingness to participate is low, the choices of data users and the government will inevitably be (illegal use, low investment in regulation). Only when individuals choose to participate can the personal data value chain be sustained. At the same time, equilibrium point analysis confirms the "privacy paradox" phenomenon; when individuals perceive that the social environment is unable to protect their data rights and interests, they will still choose to participate in order to gain certain benefits to offset the losses from personal data leakage.
2. For individuals, the main factors influencing their strategic behavior are the benefits of data services, participation costs, and the risks of privacy leakage. As the benefits of data services increase, individuals are more likely to participate. However, when participation costs and privacy leakage risks rise, individuals tend to choose "non-participation". The trust benefits that data users bring through compliance are secondary factors influencing individuals' strategic choices. This is likely because, compared to explicit benefits like data service rewards, the implicit trust benefits have less appeal for individuals.
3. For data users, the economic benefits derived from utilizing personal data, the additional costs of compliant use, the profits from data abuse, and the fines for non-compliance are the key factors affecting their strategy choices. Data users are driven

to develop data services to maximize economic benefits, and the greater the potential profits, the stronger their motivation to provide personal data services. Nevertheless, when the costs of compliant use are excessively high, data users may be tempted to use data non-compliantly due to speculative psychology. At this point, increasing the penalties for data abuse can encourage them to revert to compliant use.

4. For the government, the primary factors influencing its strategy choices are social benefits and the additional costs of high regulatory investment. Achieving greater social benefits is not only the government's ultimate goal, but it also enhances the expectations and positivity of individuals and data users regarding future gains, thereby boosting their enthusiasm. However, the higher the government's regulatory costs, the lower its willingness to continue investing such high costs. The government needs to dynamically balance the regulatory costs with the social benefits achieved.

6.2. Policy Recommendations

Based on the above research findings, this paper puts forward the following suggestions:

Enhance the Guiding Role of Application Scenarios: The realization of personal data value depends on data classification, grading governance, and improved standardization in specific scenarios. This meets user needs and boosts data utilization and industrial development. Measures like data catalogs and sandbox testing can enhance standardization and test application scenarios. Data catalogs, listing shareable data metadata, help users understand data for better decision-making and reduced error risks. Sandbox testing allows for trial-running data in controlled environments before real-world application. Financial, medical, and other data-rich institutions should collaborate, with government support, to build platforms similar to South Korea's MyData. This expands personal data circulation, enriches application scenarios, and benefits people.

Advance the Construction of Trustworthy Personal Data Spaces: High privacy risks can hinder data sharing. Trustworthy data spaces, with integrated systems like technology and standards, lower leakage and abuse risks. Technically, blockchain and privacy computing are vital for secure data transmission and use. Legally, laws like the Cybersecurity Law and the Personal Information Protection Law regulate data handlers, ensuring data security and reasonable utilization. This also facilitates supervision, reduces regulatory costs, and effectively manages data risks through full-lifecycle oversight.

Explore and Improve Personal Data Revenue-Sharing Mechanisms: Personal data revenue sharing is crucial for data value realization. Personal benefits are key to ensuring sustainable data value chains. Offer free basic data services like queries and management. Economically, investigate personal needs for value-added services to boost their income. Data users can profit from technical charges or ads, like API development or personalized financial services. In the initial stage, the government can cover fees. Later, charge based on data flow and API calls, with regular cost updates.

Strengthen the Management of Data Users: Data abuse can lead to non-compliance. A closed-loop governance with rules, technology, supervision, and punishment is needed. Promote data-usage transparency via blockchain for data security and operation recording, reducing illegal gains. Given numerous data users, establish public supervision with whistleblower systems and rewards for reported cases. Penalize data abuse by listing violators in public blacklists linked to central bank credit systems, affecting loans and bids. This deters violations and promotes the healthy development of industries related to personal data.

6.3. Limitations and Further Research

Based on the analysis of the personal data collection and development process, this study abstracts three main stakeholders—individuals, data users, and the government—and establishes a tripartite evolutionary model. It provides valuable insights into the mutual influence of decision-making behaviors among relevant parties in the circulation and utilization of personal data, also offering theoretical support for government decision-making. However, this paper primarily concentrates on theoretical exploration, and the recommendations offered serve mainly as theoretical guidance for personal-data-sharing practice. Future research will adopt a data-value-chain perspective and, drawing on both the current state of personal data value realization and empirical cases, gather firsthand evidence through interviews with the public and personal-data-sharing platforms, as well as through questionnaire surveys. Based on the interview transcripts, grounded theory and other qualitative approaches will be applied, complemented by the quantitative analysis of the survey data. These steps will enable us to refine and validate the parameters and strategies within the game model, thereby further optimizing the strategic recommendations.

Author Contributions: Conceptualization, D.W.; project administration, D.W.; writing—original draft, D.W. and J.Y.; writing—review and editing, D.W. and J.Y. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Social Science Foundation of China, grant number 23BTQ068.

Data Availability Statement: The original contributions presented in the study are included in the article, further inquiries can be directed to the corresponding author.

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

Appendix A

Table A1. Parameter Symbols and Their Meanings.

Parameter	Meaning
x	The probability of an individual choosing to participate, $0 \leq x \leq 1$
R_1	The service benefits an individual gains when choosing to participate, $R_1 > 0$
C_1	The time and effort costs of managing data when an individual chooses to participate, $C_1 > 0$
a	The probability of personal privacy leakage when data users choose to use data in compliance, $0 < a < 1$
b	The probability of personal privacy leakage when data users choose to use data in violation, $0 < a < b < 1$
L	The losses caused to individuals by privacy leakage during personal data circulation and use, $L > 0$
T	The trust benefits brought to individuals when data users use data in compliance, $T > 0$
y	The probability of data users choosing to use data in compliance, $0 \leq y \leq 1$
R_2	The total economic benefits data users gain from participating in personal data development and utilization, $R_2 > 0$
R_3	The improper benefits data users gain from overusing personal data, $R_3 > 0$
C_2	The total costs data users incur when choosing to use data in compliance, $C_2 > 0$
C_3	The total costs data users incur when choosing to use data in violation, $C_3 > 0$
k_1	The probability of data users' non-compliant use being detected, $0 < k_1 < 1$
k_2	The probability of data users' non-compliant use being detected, $0 < k_2 < 1$
F	The fine paid to the government when a data user's non-compliant use is detected
z	The probability of the government choosing high-input regulation, $0 \leq z \leq 1$
R_4	The total social benefits the government gains under a high-input regulation strategy when individuals choose to participate, $R_4 > 0$
R_5	The total social benefits the government gains under a low-input regulation strategy when individuals choose to participate, $R_5 > 0$
g_1	The regulatory costs incurred when the government chooses high-input regulation, $g_1 > 0$
g_2	The regulatory costs incurred when the government chooses low-input regulation, $g_2 > 0$

References

1. Art. 4(1) GDPR—Conditions for Consent | General Data Protection Regulation (GDPR). 2018 General Data Protection Regulation (GDPR). Available online: https://gdpr-info.eu/art-4-gdpr/ (accessed on 2 May 2025).
2. Ojasalo, J.; Miskeljin, P. Proposing a preliminary concept for a personal data ecosystem. In *INTED2020 Proceedings*; IATED: Valencia, Spain, 2020; pp. 7451–7459.
3. Kim, G.; Yoon, S. Should Personal Data Always Be Protected?: Comparison of Personal Data Utilization Policies in Foreign Countries. *J. Korean Assoc. Reg. Inf. Soc.* **2015**, *18*, 65–93.
4. Choi, W.; Chun, J.W.; Lee, S.J.; Chang, S.H.; Kim, D.J.; Choi, I.Y. Development of a Mydata Platform Based on the Personal Health Record Data Sharing System in Korea. *Appl. Sci.* **2021**, *11*, 8208. [CrossRef]
5. Evans, B.J. Barbarians at the Gate: Consumer-Driven Health Data Commons and the Transformation of Citizen Science. *Am. J. Law Med.* **2016**, *42*, 651–685. [CrossRef]
6. Hummel, P.; Braun, M.; Dabrock, P. Own Data? Ethical Reflections on Data Ownership. *Philos. Technol.* **2021**, *34*, 545–572. [CrossRef]
7. Yoon, D.; Moon, S.; Park, K.; Noh, S. Blockchain-Based Personal Data Trading System Using Decentralized Identifiers and Verifiable Credentials. In Proceedings of the 2021 International Conference on Information and Communication Technology Convergence (ICTC), Jeju Island, Republic of Korea, 20–22 October 2021; pp. 150–154.
8. Zhu, R.; Wang, M.; Zhang, X.; Peng, X. Investigation of Personal Data Protection Mechanism Based on Blockchain Technology. *Sci. Rep.* **2023**, *13*, 21918. [CrossRef]
9. Xu, L.; Liu, C. Problems and Countermeasures of Sensitive Personal Information Protection. *Inf. Stud. Appl.* **2022**, *45*, 42–49+41.
10. Sun, T.; Yuan, Z.; Li, C.; Zhang, K.; Xu, J. The Value of Personal Data in Internet Commerce: A High-Stakes Field Experiment on Data Regulation Policy. *Manag. Sci.* **2024**, *70*, 2645–2660. [CrossRef]
11. Shen, Y.; Guo, B.; Shen, Y.; Duan, X.; Dong, X.; Zhang, H. A Pricing Model for Big Personal Data. *Tsinghua Sci. Technol.* **2016**, *21*, 482–490. [CrossRef]
12. Cinnamon, J. Social Injustice in Surveillance Capitalism. *Surveill. Soc.* **2017**, *15*, 609–625. [CrossRef]
13. Janeček, V.; Malgieri, G. Commerce in Data and the Dynamically Limited Alienability Rule. *Ger. Law J.* **2020**, *21*, 924–943. [CrossRef]
14. Vandercruysse, L.; D'Hauwers, R.; Bourgeus, A. Citizen-Centric Personal Data Storage in The Public Sector: An Exploration of Opportunities, Challenges, and Preconditions. *J. Innov. Manag.* **2023**, *11*, 30–53. [CrossRef]
15. Radosevic, N.; Duckham, M.; Saiedur Rahaman, M.; Ho, S.; Williams, K.; Hashem, T.; Tao, Y. Spatial Data Trusts: An Emerging Governance Framework for Sharing Spatial Data. *Int. J. Digit. Earth* **2023**, *16*, 1607–1639. [CrossRef]
16. Asgarinia, H.; Chomczyk Penedo, A.; Esteves, B.; Lewis, D. "Who Should I Trust with My Data?" Ethical and Legal Challenges for Innovation in New Decentralized Data Management Technologies. *Information* **2023**, *14*, 351. [CrossRef]
17. Burri, M. (Ed.) *Big Data and Global Trade Law*; Cambridge University Press: Cambridge, UK, 2021.
18. Park, H.; Oh, H.; Choi, J.K. A Profit Maximization Model for Data Consumers with Data Providers' Incentives in Personal Data Trading Market. *Data* **2024**, *9*, 6. [CrossRef]
19. Pena, B.; Kursar, B.; Clarke, R.; Vines, J. Curb Your Enthusiasm: The Dissonances of Digitising Personal Finance. In *DRS Biennial Conference Series*; Design Research Society: Bilbao, Spain, 2022; Volume 67. [CrossRef]
20. Xu, Z.; Chen, X.; Hong, Y. Evolutionary Game—Theoretic Approach for Analyzing User Privacy Disclosure Behavior in Online Health Communities. *Appl. Sci.* **2022**, *12*, 6603. [CrossRef]
21. Majeed, A.; Ullah, F.; Lee, S. Vulnerability- and Diversity-Aware Anonymization of Personally Identifiable Information for Improving User Privacy and Utility of Publishing Data. *Sensors* **2017**, *17*, 1059. [CrossRef]
22. Wang, W.; Ying, L.; Zhang, J. The Value of Privacy: Strategic Data Subjects, Incentive Mechanisms and Fundamental Limits. In Proceedings of the 2016 ACM SIGMETRICS International Conference on Measurement and Modeling of Computer Science, Antibes Juan-Les-Pins, France, 15–17 June 2016.
23. Dimodugno, M.; Hallman, S.; Plaisent, M.; Bernard, P. The Effect of Privacy Concerns, Risk, Control, and Trust on Individuals' Decisions to Share Personal Information: A Game Theory-Based Approach. *J. Phys. Conf. Ser.* **2021**, *2090*, 012017. [CrossRef]
24. Wan, Z.; Vorobeychik, Y.; Xia, W.; Liu, Y.; Wooders, M.; Guo, J.; Yin, Z.; Clayton, E.W.; Kantarcioglu, M.; Malin, B.A. Using Game Theory to Thwart Multistage Privacy Intrusions When Sharing Data. *Sci. Adv.* **2021**, *7*, eabe9986. [CrossRef]
25. Zhu, F.; Song, Z. Systematic Regulation of Personal Information Rights in the Era of Big Data. *SAGE Open* **2022**, *12*, 21582440211067529. [CrossRef]
26. Zhang, Y. The Regulation of the Digital Markets. *Int. J. Educ. Humanit.* **2023**, *9*, 95–99. [CrossRef]
27. Cheong, H.; Kim, B.; Vaquero, I.U. Data Valuation Model for Estimating Collateral Loans in Corporate Financial Transaction. *J. Risk Financ. Manag.* **2023**, *16*, 206. [CrossRef]
28. Li, Z.; Liang, F.; Hu, H. Blockchain-Based and Value-Driven Enterprise Data Governance: A Collaborative Framework. *Sustainability* **2023**, *15*, 8578. [CrossRef]

29. Lrina, R.; Rob, Z.; Peter, J.V.B. Boosting Co-Opetition with Fair Sharing Approach for Inter-Organizational Information Systems. *SSRN Electron. J.* 2017, 201. Available online: https://ssrn.com/abstract=2984544 (accessed on 1 July 2025).
30. Park, J.K.; Park, S.K.; Lee, B.G. Priority of Challenges for Activation of MyData Business: K-MyData Case. *KSII Trans. Internet Inf. Syst. TIIS* **2021**, *15*, 3513–3533.
31. Oh, S.; Chung, G.; Cho, K. New Sustainable Fintech Business Models Created by Open Application Programming Interface Technology: A Case Study of Korea's Open Banking Application Programming Interface Platform. *Sustainability* **2024**, *16*, 7187. [CrossRef]
32. Alexander, J.M. Evolutionary Game Theory. In *The Stanford Encyclopedia of Philosophy*; Zalta, E.N., Ed.; Metaphysics Research Lab, Stanford University: Stanford, CA, USA, 2021; Available online: https://plato.stanford.edu/archives/sum2021/entries/game-evolutionary/ (accessed on 8 May 2025).
33. Acquisti, A.; Brandimarte, L.; Loewenstein, G. Secrets and Likes: The Drive for Privacy and the Difficulty of Achieving It in the Digital Age. *J. Consum. Psychol.* **2020**, *30*, 736–758. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.