WILEY | Hindawi

*Research Article*

# Research on Digital Information Privacy Behavior of Social Network Users Based on Evolutionary Game

**Tao Gu** [iD],[1] **Pan Zeng,**[2] **and Hua Wang** [iD][3]

[1]*School of Business Administration, Faculty of Business Administration, Southwestern University of Finance and Economics, Chengdu, China*
[2]*Planning and Development Department, Faculty of Business Administration, Southwestern University of Finance and Economics, Chengdu, China*
[3]*School of Finance, Guangdong University of Finance & Economics, Guangzhou, China*

Correspondence should be addressed to Hua Wang; wanghua1012@gdufe.edu.cn

This article takes social network services as the research object and mainly conducts two aspects of research: first, based on previous research, combining the behavior characteristics of users in the social network environment related to digital information privacy, the digital information privacy of users pays attention to the influential factors of users' digital information privacy information disclosure behavior, summarize and refine them, establish theoretical research models, and then use structural equation modelling to empirically analyze the significance of each influence path; then, based on the first part of the empirical research, the evolutionary game theory was used to analyze the interests of digital information privacy between social network users and service providers. This paper also studies the evolution of the willingness of each parameter to provide digital information to users under variable expected return conditions and uses MATLAB to analyze its evolutionary trends. It is found that the regulatory intensity coefficient, information leakage loss, and information sensitivity are both for users and websites. It has an important impact, and the loss of information leakage and information sensitivity can affect the evolution direction of users' willingness to provide digital information and change the speed of website evolution, and the regulatory intensity coefficient is the opposite.

## 1. Introduction

As social networks begin real-name registration, they are increasingly focusing on building an ecological environment with people at the center, and the stickiness and appeal of social networking sites for users are more obvious [1]. Correspondingly, the cost of obtaining personal privacy in social networks is getting lower and lower, which in turn leads to more and more attention of entrepreneurs or for-profit organizations for its commercial value [2]. However, due to the generally low security awareness and prevention skills of citizens on personal privacy in social networks, regulatory constraints, industry self-discipline, technical deficiencies,

and social credit environment [3] are not yet perfect, resulting in some illegal individuals or organizations driven by interests using improper means to illegally collect, sell, disseminate, develop, and utilize personal privacy in social networks, which seriously threaten the security of personal privacy in social networks [4, 5].

Judging from the existing research, the research on personal "information privacy" and "privacy concerns" has a long history [6–9]. As we all know, "information privacy" is an interdisciplinary and crossdomain concept. Scholars in different fields such as management, sociology, psychology, and law have studied from different theoretical perspectives and put forward related concepts and connotations

[10]. With the inference attack on relating information in social networks, Ignatenko proposed that users and social network service providers should pay attention to the setting of group relationships and friend relationships in social networks [11]. Ning et al. analyzed the antecedents, and influencing results will be reduced due to the higher degree of privacy importance [12]. Hodkinson used the theory of evolutionary game to study the relationship between privacy, trust, and cooperation in shopping websites [13]. Logesh and Subramaniyaswamy used evolutionary game theory to analyze the promotion of government immunization programs [14]. Through research, they found that group dynamic learning and imitation capabilities in game theory can play an important role in the popularization of vaccine projects and the willingness of people to vaccinate [15, 16]. Vanderhoven et al. used evolutionary game theory to study the formation mechanism of unified decision opinions [17]. Through the establishment of a game model, simulation software was used to simulate the strategic selection of question participants in the discussion process [18, 19]. In addition, Joo and Teng used evolutionary game theory to study the conflicts of interest and cooperation in society from the perspective of dynamic learning [20]. By establishing a dynamic learning model to analyze the evolutionary stable state of the game process, it was found that conflicts and the cooperation problem have different evolutionary tendencies under different conditions [21]. Finally, the author puts forward relevant strategies and suggestions to make this kind of problem develop in a direction that is beneficial to society [22]. Through combing and analyzing the previous studies, it is found that the previous research on the private paradox has mainly focused on the same behavior of the current interests of both parties.

Palos Sánchez et al. studied and summarized the information dissemination and recommendation mechanism in social networks [23] and constructed a game model of information dissemination on social networks. Through the establishment of the evolutionary game model of both parties, they conducted an in-depth analysis of the customers and enterprise's interest relationship and dynamic evolutionary process under different strategies, influencing factors, and evolutionary path of the integrity problem in e-commerce websites. Privacy issues cannot be properly resolved, and the development of LBS sign-in services will likely enter a bottleneck period, thereby greatly limiting the rapid development of user scale and ultimately damaging the interests of all parties.

Through the research on the factors that affect the privacy of social network users, the factors that affect privacy disclosure, and the long-term dynamic game behavior between users and service providers, on the one hand, they can discover the important factors that affect users' privacy behaviors in the social network environment and further explain users and social network and the long-term evolution of the privacy interests of the online community, so as to indicate the direction and provide practical policy recommendations for the long-term development of social network service providers; on the other hand, it further broadens the research scope of evolutionary game theory and provides a new method for studying social networks. Therefore, this study will use evolutionary game theory to treat users and social network service providers as two interacting groups and, on the basis of the first part of empirical research, introduce the influencing factors of emergencies by constructing a revenue matrix and replicators. Dynamic equations are used to obtain an evolutionary game model of the private benefit game.

## 2. Method

*2.1. Construction of Factors Affecting Digital Information of Social Network Users.* According to social exchange theory, people will dominate their behaviors in pursuit of maximizing their own interests. These decision-making behaviors depend on the measurement of their own gains and losses, including the rewards and risks they receive. The core of the theory is that the interacting parties follow the principle of reciprocity. When their expected benefits are greater than the cost, the exchange occurs. Among them, the exchange gains include not only material gains but also psychological gains. When analyzing the user's digital information from the perspective of social exchange theory, the behavior can also be regarded as the decision-making process of the user's exchange behavior. Users' trust in service providers and members provides personal information in exchange for communication with other members and online information and also reduces the willingness to disclose information because of the importance of privacy. When this process has a positive effect, the user's willingness to provide increases, and conversely, the willingness to provide decreases.

As an indispensable tool for users to contact friends and engage in entertainment interactions, social networks also worry about the use of their information by service providers while they are enjoying the digital experience, causing them to worry about their own information. This seriously affects the user experience and causes user churn. Based on the existing research on social networks, this paper extracts the factors that affect users' digital information from the perspective of users, social networking sites, and network environment.

(1) User perspective

*Privacy is important*: privacy emphasis refers to the possible information leakage caused by users disclosing their information to others. The fear of losing privacy is the user's subjective perception of the possibility of their own information leakage. In the Internet age, users will pay attention to privacy when filling in registration-related information on the website. With the popularity of social media, users have greater concerns about their own information (personal photos, accounts, and preferences) and other security issues, especially for mobile service applications. The focus on location privacy has also gradually increased. Users' concerns about privacy are mainly about the misuse of information and the illegal acquisition and sale of third parties. Some scholars have shown through research that privacy attaches a

negative correlation to users' willingness to disclose digital information in the online environment, and some studies have proved that with user privacy, the increased attention will reduce the willingness of online users to disclose behaviors; that is, the greater the negative impact or loss of online users, the more negative the willingness to disclose information.

*Trust index*: the trust index refers to the individual's total wish to depend on others and is determined by the individual's own characteristics, growth background, and development experience. The individual's trust index can affect the user's trust in the website. The mobile Internet is virtual and unstable, which enhances the risk of user behavior. Trust can reduce the perceived risk of users, thereby increasing their willingness to disclose their information.

*Experience feelings*: experiential feelings were originally applied to psychology, which refers to individuals devoting themselves to an activity and ignoring the surrounding environment. Most are measured from the perspective of perceiving entertainment and emotional support. In a social network environment, perceived entertainment performance is the user's happy experience and enjoyment when using the application; emotional support is the user's emotional response to the product or service consumption experience. Emotional support obtained is the emotional care or help obtained by communicating with others and psychological comfort. In order to obtain the encouragement and help of others, it affects personal attitudes and thus affects the user's decision-making. When in the state of experiencing feelings, attention is drawn and has an impact on the user's attitude and behavior.

*Perceived information controlled*: it refers to the ability of individuals to control their information when it is released, including some private settings. Users with strong information control ability have better choices and judgments about their own information, which can be disclosed and which is private to maximize protection from infringement, which can reduce their concerns when using the network.

(2) Social network perspective

*Reputation of social networking sites*: in a social network environment, the reputation of a website refers to the public, that is, the user's perception of the website's concern, integrity, and the degree of fulfilment of the agreement. The higher the reputation of the website, the more the user trusts the website, which affects the user's disclosure of relevant information to the website they trust.

*Social network security*: the website adopts corresponding protection measures, high-level technical support, from the user's perspective; for the user's information security considerations, the user will be willing to believe that the website's service is well-intentioned and reliable within a certain range, so as to provide a positive attitude. Provide corresponding information. If the website does not provide users with corresponding protection measures to ensure that users' digital information will not be maliciously bought or used, users will not be able to obtain the corresponding goodwill perception, which will reduce their willingness to disclose their own information.

*Privacy policy of social networking sites*: privacy policies have an important impact on users' privacy concerns. Privacy policies can make users feel more secure and assured. Privacy policies can negatively affect privacy concerns, which in turn increase user digital information disclosure.

(3) Network environment perspective

*Ease of use of social networking sites*: according to the previous understanding of the concept of ease of use, coupled with the characteristics of the Internet, this article believes that the ease of use of the website is a degree to which users can feel the ease of operation and easy understanding within the website, and also includes future learning and use in the future. The website requires a sense of effort and time. When the user feels complicated to provide more information when registering and it takes longer time, it will reduce the user's willingness to provide information; if the website is not set up reasonably and the operation cannot be simple and convenient, it will affect the user's enthusiasm to participate in the website. As a result, users' willingness to provide digital information is reduced, and users are even lost.

*Usefulness of social networking sites*: website usefulness refers to the utility of the website that users can feel when they participate in the website. This kind of utility is not only the concessions and rewards given but also the validity, usefulness, and comfort of the information. Nowadays, the most important thing in society is personalized customization. The disclosure of personal information by users extends from the initial material rewards to the service output today. The website can provide users with high-quality services. Users naturally hope that the website can provide more and more comprehensive information for themselves. The strength of the user's willingness to provide digital information will be affected by the user's perceived size of the sites expected utility. The greater the perceived utility, the stronger the willingness; otherwise, the weaker.

*Involvement of social networking sites*: it refers to the time and effort invested by the user in using the website, adding the site involvement degree in the TAM model, and verifying that the user's willingness to use is directly affected by the site involvement degree. There is a correlation between involvement and use digital information. The higher the involvement of the user on the website, the more willing to answer the personal information questions raised by the website.

*User digital information sensitivity*: it refers to the extent to which the information provided by the user to others has been leaked and harmed. Generally, similar information has different sensitivity to different individuals, that is, the sensitivity of information varies from person to person. The sensitivity of users' digital information has a negative impact on their willingness to provide information. The higher the sensitivity of the information, the greater the risk perceived by the user, and the more difficult it is to provide. The sensitivity of the same user to the same information is also different in different situations. For example, the sensitivity of location information when shopping on a website is lower than that on social networking sites.

TABLE 1: User digital information influence factor system.

| Type of influence | Influence factor | Factor sign |
|---|---|---|
| User perspective | Private value | $f_1$ |
| | Trust index | $f_2$ |
| | Experience feeling | $f_3$ |
| | Perceptual information control | $f_4$ |
| Social network perspective | Social network reputation | $f_5$ |
| | Social network security | $f_6$ |
| | Privacy policy of social networking sites | $f_7$ |
| Network environment perspective | Ease of use on social networking sites | $f_8$ |
| | Usefulness of social networking sites | $f_9$ |
| | Social network involvement | $f_{10}$ |
| | User digital information sensitivity | $f_{11}$ |

According to the above analysis, the establishment of user information digital information influencing factor system is shown in Table 1.

### 2.2. Identification and Analysis of Factors Affecting Digital Information of Social Network Users.

Twelve survey respondents including college experts, website operation experts, and network users are selected for scoring, and the subjectivity of expert scoring is reduced by introducing fuzzy set theory. DE blur the expert score and convert the ternary fuzzy number into a more accurate number, so as to obtain the precise value of the interaction between various factors. The obtained 8 questionnaires are transformed by linguistic variables and ternary fuzzy numbers, and the conversion relationship is shown in Table 2.

Set the ternary fuzzy number corresponding to the judgment result as formula (1), and perform diversification on the ternary fuzzy number.

$$O\left(O_{ij}^k, P_{ij}^k, Q_{ij}^k\right), \quad i(j) = 1, 2 \cdots \cdots 11, k = 1, 2 \cdots \cdots 12. \quad (1)$$

Standardize the ternary fuzzy numbers evaluated by experts to reduce the subjectivity of the judges.

$$fO_{ij}^k = \frac{O_{ij}^k - \min_{1 \le k \le K} O_{ij}^k}{\max_{1 \le k \le K} Q_{ij}^k - \min_{1 \le k \le K} O_{ij}^k},$$

$$fP_{ij}^k = \frac{P_{ij}^k - \min_{1 \le k \le K} O_{ij}^k}{\max_{1 \le k \le K} Q_{ij}^k - \min_{1 \le k \le K} O_{ij}^k}, \quad (2)$$

$$fO_{ij}^k = \frac{Q_{ij}^k - \min_{1 \le k \le K} O_{ij}^k}{\max_{1 \le k \le K} Q_{ij}^k - \min_{1 \le k \le K} O_{ij}^k}.$$

Second, calculate the standard value, according to the following formula (3) and formula (4) into the left and right

TABLE 2: Correspondence between linguistic variables and ternary fuzzy numbers.

| Linguistic variables | Ternary fuzzy number |
|---|---|
| Serious impact | (0.7, 0.9, 1.0) |
| More serious impact | (0.5, 0.7, 0.9) |
| General impact | (0.3, 0.5, 0.7) |
| Minor impact | (0.1, 0.3, 0.5) |
| Almost no effect | (0, 0.1, 0.3) |

standard values, and then calculate the total standard value according to formula (5).

$$fOs_{ij}^k = \frac{fP_{ij}^k}{1 + fP_{ij}^k - fO_{ij}^k}, \quad (3)$$

$$fQs_{ij}^k = \frac{fQ_{ij}^k}{1 + fQ_{ij}^k - fO_{ij}^k}, \quad (4)$$

$$f_{ij}^k = \frac{fOs_{ij}^k\left(1 - fOs_{ij}^k\right) + fQs_{ij}^k fQs_{ij}^k}{1 - fOs_{ij}^k + fQs_{ij}^k}. \quad (5)$$

Finally, the last step is complete blurring. The calculation of the influence value of $i$ factor given by each expert on $j$ factor is based on formula (6); then, the average influence value of the expert group is calculated according to formula (7).

$$a_{ij}^k = \min_{1 \le k \le K} O_{ij}^k + f_{ij}^k\left(\max_{1 \le k \le K} Q_{ij}^k - \min_{1 \le k \le K} O_{ij}^k\right), \quad (6)$$

$$a_{ij}^k = \frac{1}{k}\sum_{k=1}^{k} a_{ij}^k. \quad (7)$$

TABLE 3: Direct influence matrix $A_{N*N}$ of factors affecting digital information of network users.

| Factor | $f_1$ | $f_2$ | $f_3$ | $f_4$ | $f_5$ | $f_6$ | $f_7$ | $f_8$ | $f_9$ | $f_{10}$ | $f_{11}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $f_1$ | 0 | 0.645 | 0.605 | 0.631 | 0.681 | 0.679 | 0.617 | 0.523 | 0.576 | 0.632 | 0.624 |
| $f_2$ | 0.724 | 0 | 0.536 | 0.523 | 0.556 | 0.488 | 0.578 | 0.457 | 0.555 | 0.594 | 0.416 |
| $f_3$ | 0.412 | 0.616 | 0 | 0.423 | 0.53 | 0.447 | 0.599 | 0.386 | 0.521 | 0.579 | 0.461 |
| $f_4$ | 0.453 | 0.528 | 0.417 | 0 | 0.329 | 0.364 | 0.475 | 0.546 | 0.532 | 0.43 3 | 0.467 |
| $f_5$ | 0.482 | 0.539 | 0.449 | 0.529 | 0 | 0.745 | 0.682 | 0.581 | 0.69 | 0.458 | 0.426 |
| $f_6$ | 0.434 | 0.439 | 0.432 | 0.642 | 0.546 | 0 | 0.745 | 0.457 | 0.523 | 0.429 | 0.318 |
| $f_7$ | 0.362 | 0.415 | 0 45 | 0.415 | 0.521 | 0.489 | 0 | 0.517 | 0.464 | 0.449 | 0.334 |
| $f_8$ | 0.428 | 0.451 | 0.421 | 0.451 | 0.434 | 0.46 | 0.44 | 0 | 0.442 | 0.442 | 0.381 |
| $f_9$ | 0.44 6 | 0.456 | 0.433 | 0.574 | 0.424 | 0.378 | 0.454 | 0.841 | 0 | 0.405 | 0.446 |
| $f_{10}$ | 0.642 | 0.657 | 0.457 | 0.562 | 0.452 | 0.445 | 0.411 | 0.473 | 0.468 | 0 | 0.346 |
| $f_{11}$ | 0.691 | 0.633 | 0.716 | 0.692 | 0.723 | 0.454 | 0.396 | 0.437 | 0.674 | 0.7.2 | 0 |

TABLE 4: Values of $D$, $R$, $D + R$, and $D - R$ affecting the user's digital information.

| Factor | $D$ | $R$ | $D + R$ | $D - R$ |
|---|---|---|---|---|
| $f_1$ | 1.4449 | I.0364 | 2.4913 | 0.6184 |
| $f_2$ | 1.1843 | 1.1908 | 2.3741 | -0.0064 |
| $f_3$ | 1.0034 | 0.9868 | 1.9902 | 0.0166 |
| $f_4$ | 0.8433 | 1.176 | 2.0293 | -0.3227 |
| $f_5$ | 1.2224 | 1.1476 | 2.3701 | 0.0749 |
| $f_6$ | 0.9144 | 0. 9698 | 1.8842 | -0.0444 |
| $f_7$ | 0.7424 | 1.1226 | .1.874 | -0.3702 |
| $f_8$ | 0.7303 | 1.0384 | 1.6688 | -0.3082 |
| $f_9$ | 0.9008 | 1.2377 | 2.1384 | -0.3369 |
| $f_{10}$ | 0.9972 | 1.0827 | 2.0799 | -0.0844 |
| $f_{11}$ | 1.6648 | 0.7894 | 2.4443 | 0.8743 |

Record the values in the $11 * 11$ matrix as shown in Table 3 to obtain the direct impact matrix:

$$A_{N*N} = \left[ f_{ij} \right]_{11*11}, \quad i(j) = 1, 2 \cdots \cdots 11 ; i = j, f_{ij} = 0. \quad (8)$$

In this paper, the direct influence matrix $A_{N*N}$ is converted into a standardized influence matrix $B_{N*N}$ according to formula (9) and then into the comprehensive influence matrix $C_{N*N}$ according to formula (10):

$$B_{N*N} = \frac{1}{\max \sum_{j=1}^{11} f_{ij}} A_{N*N}, \quad (9)$$

$$C_{N*N} = B_{N*N} (1 - B_{N*N})^{-1}. \quad (10)$$

The comprehensive influence matrix $C_{N*N}$ is obtained, and then, sum each row and each column, according to the MATLAB solution; the influence degree, influence

degree, centrality, and cause degree of each influence factor are shown in Table 4.

2.3. Construction of the Evolutionary Game Model of Social Network User Digital Information. Social network is different from the general network, not only to meet the user's personalized service need but also to meet the user's emotional needs, so that users can search for people, things, and information related to themselves in a timely manner. Most of the revenue of social networks comes from advertising. The main forms of advertising include interactive games, user reviews, value-added services with advertisements, and e-mail. Therefore, it is assumed that the social network provides accurate marketing by obtaining user information, and the additional income obtained is $W_1$.

For users, users need to register and post opinions to participate in games and comments. Posting comments involve personal personality, attitudes, preferences, and friends. Therefore, when users provide "privacy" information to the website, they obtain information and services recommended by the website based on the user's interests and behavior. These include personalized recommendation services provided by the website and access to virtual currency, so that users can obtain relevant product information within a short time by browsing the page, which is beneficial to users to save time, reduce the benefits of search costs, and enjoy the cooperation of merchants through geographic location information, external benefits such as consumer discounts; in addition, unlike other virtual communities, in social networks, users more want to get social emotional needs. Social networks are interactive. In social networks, users can establish contact with relatives, friends, and strangers to obtain internal benefits such as pleasure and emotional support. Therefore, external and internal benefits obtained by users are assumed to be $B_1$ and $B_2$, respectively. Therefore, it is assumed that the loss suffered by the user from the privacy invasion leakage is $L$. The loss of private information leakage is affected by the sensitivity of the information. Therefore, the information sensitivity coefficient $\beta$ is set to balance the size of the information leakage loss.

TABLE 5: Model path estimates and test values.

| Path | Estimate | S.E. | C.R. | $p$ |
|---|---|---|---|---|
| Privacy concern (adverse events of others) | 0.226 | 0.046 | 2.879 | 3.005** |
| Privacy concerns | 0.145 | 0.064 | 2.324 | 5.126* |
| Privacy concern (personal adverse events) | 0.352 | 0.071 | 0.513 | *** |
| Privacy concern (personal media exposure) | 0.206 | 0.053 | 4.176 | 2.018** |
| Privacy concern (network literacy) | 1.067 | 1.246 | 1.437 | 1.114 |
| Willingness to act (privacy concerns) | -0.345 | 0.433 | -3.916 | 0.005** |
| Willingness to act (external revenue) | 6.623 | 7.269 | 8.013 | ** |
| Willingness to act (internal income) | 2.981 | 3.157 | 3.236 | 0.003** |

* means $p < 0.05$, ** means $p < 0.01$, and *** means $p < 0.001$.

TABLE 6: Model fit index.

| Fitting index | CMIN/DF | RMR | RMSEA | GFI | CFI | NFI | IFI |
|---|---|---|---|---|---|---|---|
| Model fitting value | 0.165 | 0.121 | 0.069 | 0.856 | 0.912 | 0.987 | 0.945 |
| Acceptable recommended value | Close to 0 | < 0.05 | < 0.1 | > 0.9 | > 0.9 | > 0.9 | > 0.9 |

TABLE 7: Confirmatory factor analysis test.

| Type of influence | Factor sign | Factor load | Cronbach's $\alpha$ | Combined reliability | Average extractor |
|---|---|---|---|---|---|
| User perspective | $f1$ | 0.799 | 0.860 | 0.862 | 0.613 |
| | $f2$ | 0.858 | | | |
| | $f3$ | 0.777 | | | |
| | $f4$ | 0.689 | | | |
| | $f5$ | 0.70 1 | | | |
| Social network perspective | $f6$ | 0.833 | 0.819 | 0.834 | 0.627 |
| | $f7$ | 0.835 | | | |
| | $f8$ | 0.759 | | | |
| Network environment perspective | $f9$ | 0.759 | 0.852 | 0.852 | 0.591 |
| | $f10$ | 0.778 | | | |
| | $f11$ | 0.778 | | | |

TABLE 8: Values of various parameters.

| Happening | $B_1$ | $B_2$ | $B_3$ | $L$ | $W_2$ | $C$ | $R$ | $\alpha$ | $\beta$ | $\gamma$ |
|---|---|---|---|---|---|---|---|---|---|---|
| Situation A | 1.5 | 2.5 | 1 | 2 | 4.5 | 4 | 2.5 | 0.5 | 0.5 | 1 |
| Case B | 1.5 | 2.5 | 1 | 1 | 4.5 | 4 | 1 | 0.5 | 0.5 | 1 |
| Case C | 1.5 | 2.5 | 1 | 2 | 3.5 | 4 | 2.5 | 0.5 | 0.5 | 1 |
| Situation D | 1.5 | 2.5 | 1 | 1 | 3.5 | 4 | 1 | 0.5 | 0.5 | 1 |

During the operation of the website, the website is subject to the supervision of the government regulatory department, and the degree of supervision of the regulatory agency can affect the user's willingness to provide information. Some researchers have shown that users believe that the government maintains the network order and reduces the risk of privacy leakage. The higher the regulatory intensity, the higher the trust level, and the higher the user's security perception benefit $B_3$. Similarly, the higher the supervision intensity, the more the user trusts the website, and user participation will increase accordingly. This will undoubtedly increase the website revenue. In this article, it is assumed that this part of the revenue is the trust revenue $W_2$ obtained by the website, so it is also subject to the supervision department regulatory strong impact. At the same time, it can also affect the input cost of website information protection. In order to avoid the penalty imposed by the regulatory agency, the website will choose its own cost of information protection $C$ according to the intensity of the supervision. When the supervision intensity is weak, the user will save money. Information protection measures are also relatively scarce, and the standards for software and hardware updates and privacy policies of the website are reduced. On the contrary, when the intensity of supervision is strong, the website will choose to increase costs to protect user information in order to avoid greater loss of profits. Therefore, the cost of the website is also

affected by the intensity of regulation. When the website does not protect user information, the website participation rate will gradually decrease, causing the loss of the website to be assumed to be R. According to the stability theorem of differential equations, the evolutionary game model of willingness to provide information between socially connected users and websites can be expressed by the following two differential equations:

$$G(x) = \frac{d_{x(t)}}{d_t} = x(1 - x) * [y\alpha B_3 + B_1 + B_2 - \beta L + y\beta L],$$

(11)

$$G(y) = \frac{d_{y(t)}}{d_t} = y(1\text{-}y) * [\alpha W_2 - \alpha Cx - \alpha W_2 + x\beta\gamma L + xR].$$

(12)

For an evolutionary game model, the equilibrium point obtained by the two sides of the game according to the dynamic replication equation is not necessarily the equilibrium point of the system. The system's stabilization strategy must be composed of both parties of the game. Social network users and social networking sites together constitute. According to the equations formed by the dynamic equations of social network users and websites, the five equilibrium points of the system can be obtained as A (0, 0), B (1,0), C (0, 1), D (l, L), and E(x∗,). The local stability of the system can be derived based on the local stability of the Jacobian matrix. If the evolutionary equilibrium point of the system can satisfy the Jacobian matrix, the equilibrium point can be derived as the evolutionary stable strategy. The evolution of the selection strategy of social networking sites and their users can be described by the system composed of the above equations (11) and (12). The Jacobian matrix of this system is

$$J = \begin{bmatrix} (1 - 2x)[y\alpha B_3 + B_1 + B_2 - \beta L + y\beta L] & x(1 - x)[\alpha B_3 + \beta L] \\ y(1 - y)[R + y\beta L - \alpha W_2] & (1 - 2y)[\alpha W_2 - \alpha Cx - \alpha W_2 + x\beta\gamma L + xR] \end{bmatrix}.$$

(13)

## 3. Results

*3.1. Data Path Analyses.* Import preprocessed sample data into the AMOS data set, estimate and test the path coefficients in the research model, and finally obtain the estimated value and significant index of each path coefficient, as shown in Table 5. It can be seen from Table 4 that the negative media exposure (GME), personal negative media exposure (PME), personal adverse event experience (PBE), and other person's adverse event experience (GBE) experienced by privacy concerns (PC) have a positive impact; personal network literacy improvement (NL) has no effect on user privacy concerns (PC); external revenue perception (ER) and internal revenue perception (IR) have positive effects on behavioral will (BI).

At the same time, the analysis report output by AMOS yields the model fit index, as showed in Table 6. It is generally believed that if the model fit can better meet the relevant standards. It indicates that the research model matches the data. A well-built model is more reasonable, and the estimated value of the path coefficient will be more meaningful. Generally speaking, the closer CMIN/DF is to 0, the better the adaptability of the model to the data. The CMIN/DF value of the model in this study is 0.16, so the model has a good match with the data. In addition, the RMR, RMSEA, CFI, NFI, IFI, and other indicators all meet the relevant judgment criteria. Although GFI index value of the model is 0.897, which does not meet its judgment criteria, its value is closer to 0.9, and other relevant indicators can meet the requirements very well. Therefore, the model of this study is considered to have a good fit.

*3.2. Analysis of Private Behavior.* Reliability (reliability) test refers to measuring the reliability of data by studying the consistency, stability, and reliability of test data and results. The factor load of each dimension is between 0.670 and 0.884, and all reach the standard range (more than 0.6; those less than 0.6 are deleted). Specific values are shown in Table 7.

*3.3. Simulation Analyses of Evolutionary Model.* According to the actual situation, it is assumed that the cost C of protecting user information on the website is the utility of 4 units and uses this as a reference to assign values to each parameter. The assignment is shown in Table 8.

Figure 1 is the evolutionary simulation of four cases. As can be seen in Figure 1(a), x and y both gradually approached 1 and stabilized from 0.3, indicating that the evolutionary stability result of Game A is (providing, protecting), which is consistent with the simulation results. As can be seen in Figure 1(b), x gradually tends to 1 from 0.3 and finally reaches stability at 1; y gradually tends to 0 from 0.3 and finally approaches 0 at infinity and reaches a stable state, indicating that Case B simulation results are (provided, not protected), which is completely consistent with the previous system evolution analysis results. As can be seen in Figure 1(c), x and min gradually approached 1 from 0.3 and eventually reached a stable state. Compared with the website, users reach a stable speed faster. The simulation result is (provide, protect), which is consistent with the evolutionary stability analysis result. Compared with Case A, changing the size relationship between the website's perceived revenue and website protection information cost
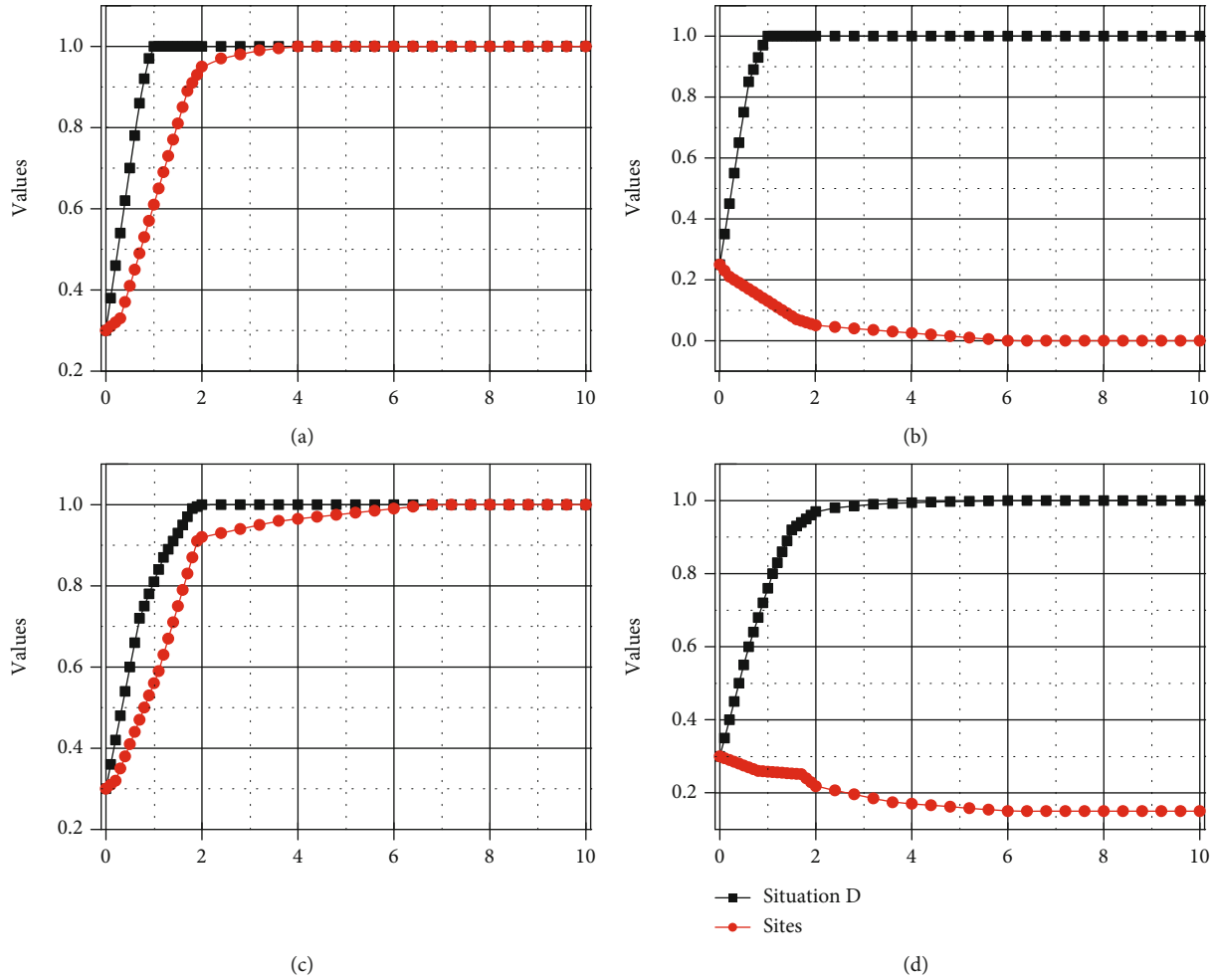
(a)

(b)

(c)

(d)

Figure 1: Simulation results.

investment has no effect on the system's evolutionary stability results, only the evolutionary stable speed. As showed in Figure 1(d), $x$ gradually approached from 0.3 to 1, while $y$ approached downward from 0.3 and gradually approached 0 and eventually reached stability, indicating that the simulation result is (provided, not protected). The simulation results under this condition are consistent with the evolutionary analysis. It can be seen from the results of the numerical simulation of the above four cases that the simulation results are completely consistent with the results of the previous model evolutionary stability analysis, indicating the correctness of the model.

## 4. Discussion

Nowadays, social networks are in the golden period of development. Social networks are gradually changing the way of life and work of the current society. The mobile social network has become an irreversible trend, and the "double-edged sword effect" of personalized services is also urgently needed. Due to the limitations of personal capabilities, the number of interviewed groups and the number of samples in this survey are limited, and the relevant results cannot be better. To explain the actual situation, it is necessary to

continue to investigate the specific content of personal privacy in social networks in more depth. In the future, we should continue to deeply analyze each relevant clause in the current laws and regulations and research and put forward specific rules and suggestions for the specific content of personal privacy in the social network of the contemporary information society.

## 5. Conclusion

This paper mainly studies the influencing factors of digital information private behavior of social network users and the analysis of the game process with service providers. First, the method of questionnaire survey and structural equation model is used for empirical data analysis. The conclusion finds a significant role in influencing factors of privacy concerns and behavioral intentions of social network users, proving that the emergencies experienced by users and environmental factors of external groups will positively affect the user's privacy concern level, and the user's privacy concern and perceived benefits will also significantly affect their privacy information disclosure behavior intentions. First, the DEMATEL method is applied to the research on the influencing factors of users 'digital information. The

conclusion finds the key influencing factors of users' digital information. Based on the combination of the user's perceived revenue and risk perception, the key influencing factors affecting their digital information establish the influence through the evolutionary game theory. The evolutionary game model of user digital information analyzes the changing rules of user digital information in different situations. In the future, we should consider taking out the third-party regulators separately and establishing an evolutionary model of the game between network users, network service providers, and regulators.

## Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

## Conflicts of Interest

The authors declare that they have no conflicts of interest.

## Acknowledgments

## References

[1] J. Du, C. Jiang, and E. Gelenbe, "Distributed data privacy preservation in IoT applications," *IEEE Wireless Communications*, vol. 25, no. 6, pp. 68–76, 2018.

[2] C. Jiang, L. Kuang, Z. Han, Y. Ren, and L. Hanzo, "Information credibility modeling in cooperative networks: equilibrium and mechanism design," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 2, pp. 432–448, 2017.

[3] M. Walrave, K. Poels, M. L. Antheunis, E. van den Broeck, and G. van Noort, "Like or dislike? Adolescents' responses to personalized social network site advertising," *Journal of Marketing Communications*, vol. 24, no. 6, pp. 599–616, 2018.

[4] K. Argasinski and M. Broom, "Interaction rates, vital rates, background fitness and replicator dynamics: how to embed evolutionary game structure into realistic population dynamics," *Theory in Biosciences*, vol. 137, no. 1, pp. 33–50, 2018.

[5] L. Kelly, G. Kerr, and J. Drennan, "Privacy concerns on social networking sites: a longitudinal study," *Journal of Marketing Management*, vol. 33, no. 17-18, pp. 1465–1489, 2017.

[6] E. L. Spottswood and J. T. Hancock, "Should I share that? Prompting social norms that influence privacy behaviors on a social networking site," *Journal of Computer-Mediated Communication*, vol. 22, no. 2, pp. 55–70, 2017.

[7] W.-L. Shiau, Y. K. Dwivedi, and H. S. Yang, "Co-citation and cluster analyses of extant literature on social networks," *International Journal of Information Management*, vol. 37, no. 5, pp. 390–399, 2017.

[8] W. Wei, S. Liu, W. Li, and D. du, "Fractal intelligent privacy protection in online social network using attribute-based encryption schemes," *IEEE Transactions on Computational Social Systems*, vol. 5, no. 3, pp. 736–747, 2018.

[9] C. Smith, J. Brock Smith, and E. Shaw, "Embracing digital networks: entrepreneurs' social capital online," *Journal of Business Venturing*, vol. 32, no. 1, pp. 18–34, 2017.

[10] J. Huang, S. Kumar, and H. Chuan, "Gender differences in motivations for identity reconstruction on social network sites," *International Journal of Human–Computer Interaction*, vol. 34, no. 7, pp. 591–602, 2018.

[11] O. P. Ignatenko, "Game theoretic modeling of AIMD network equilibrium," *Problems IN Programming*, vol. 1, no. 4, pp. 116–128, 2018.

[12] Z. Ning, F. Xia, N. Ullah, X. Kong, and X. Hu, "Vehicular social networks: enabling smart mobility," *IEEE Communications Magazine*, vol. 55, no. 5, pp. 16–55, 2017.

[13] P. Hodkinson, "Bedrooms and beyond: youth, identity and privacy on social network sites," *New Media & Society*, vol. 19, no. 2, pp. 272–288, 2017.

[14] R. Logesh and V. Subramaniyaswamy, "A reliable point of interest recommendation based on trust relevancy between users," *Wireless Personal Communications*, vol. 97, no. 2, pp. 2751–2780, 2017.

[15] F. Saab, A. Kayssi, I. Elhajj, and A. Chehab, "Playing with Sybil," *ACM SIGAPP Applied Computing Review*, vol. 16, no. 2, pp. 16–25, 2016.

[16] M. A. Ferrag, L. Maglaras, and A. Ahmim, "Privacy-preserving schemes for ad hoc social networks: a survey," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 3015–3045, 2017.

[17] E. Vanderhoven, T. Schellens, R. Vanderlinde, and M. Valcke, "Developing educational materials about risks on social network sites: a design based research approach," *Educational Technology Research and Development*, vol. 64, no. 3, pp. 459–480, 2016.

[18] W.-H. S. Tsai and L. R. Men, "Consumer engagement with brands on social network sites: a cross-cultural comparison of China and the USA," *Journal of Marketing Communications*, vol. 23, no. 1, pp. 2–21, 2017.

[19] P. E. Ketelaar, L. Janssen, M. Vergeer, E. A. van Reijmersdal, R. Crutzen, and J. van 't Riet, "The success of viral ads: social and attitudinal predictors of consumer pass- on behavior on social network sites," *Journal of Business Research*, vol. 69, no. 7, pp. 2603–2613, 2016.

[20] T.-M. Joo and C.-E. Teng, "Impacts of social media (Facebook) on human communication and relationships: a view on behavioral change and social unity," *International Journal of Knowledge Content Development & Technology*, vol. 7, no. 4, pp. 27–50, 2017.

[21] J. Knoll, "Advertising in social media: a review of empirical evidence," *International Journal of Advertising*, vol. 35, no. 2, pp. 266–300, 2016.

[22] I. Lee, "Big data: dimensions, evolution, impacts, and challenges," *Business Horizons*, vol. 60, no. 3, pp. 293–303, 2017.

[23] P. R. Palos Sánchez, J. R. Saura, A. Reyes Menéndez, and I. Vásquez Esquivel, "Users acceptance of location-based marketing apps in tourism sector: an exploratory analysis," *Journal of Spatial and Organizational Dynamics*, vol. 6, no. 3, pp. 258–270, 2018.