IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 4 July 2022, accepted 5 August 2022, date of publication 16 August 2022, date of current version 19 August 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3198705

RESEARCH ARTICLE

Tripartite Evolutionary Game of Multiparty Collaborative Supervision of Personal Information Security in App: Empirical Evidence From China

YIHANG GUO, KAI ZOU, MIAOCHENG YANG, AND CHANG LIU
School of Public Administration, Xiangtan University, Xiangtan 411105, China

Corresponding author: Kai Zou (zoukai@xtu.edu.cn)

This work was supported in part by the National Social Science Foundation of China under Grant 18BTQ055.

ABSTRACT At present, the problem of the personal information security of apps has attracted widespread attention from the government and society, and there is an urgent need for multiple subjects to participate in the regulation together. Based on this, we first considered the information feedback from users. Secondly, we constructed an evolutionary game model of three-party collaborative supervision among local governments, app distribution platforms, and users. Then the stability of the equilibrium points and their stability conditions are analyzed based on Lyapunov's first law. Finally, MatlabR2021a software is used to analyze the influence of key parameter changes on the strategy choice of game players. The conclusions are as follows: (1) Increasing the penalty amount for local governments and app distribution platforms, increasing the reputation value premium or reputation loss from users' feedback, and increasing synergistic benefits can promote local governments to adopt the strategies of supervision and app distribution platforms to adopt the strategies of review. (2) Reducing the cost of supervision for local governments can promote their adoption of supervisory strategies, and reducing the cost of review for app distribution platforms can promote their adoption of review strategies. (3) Reducing users' feedback cost not only improves users' enthusiasm to participate in supervision, but also promotes local governments and app distribution platforms to adopt positive strategies. (4) When the coefficient of synergistic benefit distribution is more even, it is more favorable for local governments and app distribution platforms to adopt positive strategies. Based on the simulation results, we propose some feasible strategies.

INDEX TERMS App, personal information security, multi-party collaborative supervision, users' feedback, evolutionary game.

I. INTRODUCTION

With the rapid development of mobile communication technology and the popularity of intelligent mobile terminal devices [1], [2], the mobile Internet economy has gradually become an important pillar supporting the prosperity of the network economy [3], [4] and has had a profound impact on the development of all areas of society [5], [6], [7], [8]. As a representative product of the mobile Internet economy [9], the variety and number of apps have shown explosive growth, not only enhancing the efficiency of data collection, storage, and exchange at the operational end [10], [11], but also becoming an essential tool for livelihood needs. In the 'State of Mobile 2022 Report' released by APP Annie, user spending on apps reached $170 billion in 2021, an increase of 19% compared to last year, and downloads continued to grow at a rate of 5% year-over-year to reach 230 billion. Obviously, the app will become the most active and mainstream form of business in the mobile market in the future, and show an irreversible trend.

Although apps are beneficial in terms of technology and services, the problems in personal information security have

The associate editor coordinating the review of this manuscript and approving it for publication was Mohamad Afendee Mohamed.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

become a new obsession. The current personal information application field is expanding, the value of personal information is being exploited [12], and users are facing the threat of personal information leakage and misuse while experiencing personalized services from apps [13], [14], [15]. Verizon's ''2020 Data Breach Development Report'' shows that 43% of data breaches are related to app vulnerabilities. Apps have gradually become a new subject of personal information leakage [16], especially the outbreak of the COVID-19 epidemic in 2020, and information security incidents such as illegal calls to personal location data and contact information through apps are becoming more frequent [17], [18], [19]. Therefore, the problem of personal information security protection of apps needs to be regulated and solved by relevant organizations urgently.

The government departments of different countries and regions have taken different measures to regulate and control the security of app personal information. In May 2018, the European Union (EU) introduced the General Data Protection Regulation (GDPR). Under the GDPR, companies (including app operators) that process the personal data of residents in the EU will need to comply with a number of privacy rules, and failure to comply with the corresponding rules will result in hefty fines. Unlike the EU, which has strict top-down legislation to protect the personal information security, the United States (US) is against comprehensive supervision of privacy or data based on the consideration of promoting economic development [20]. Currently, there is no uniform bill to protect personal information security in effect at the federal level in the US, and only the ''Draft App Privacy Protection and Security Act'' was released in 2018 in an attempt to achieve a dynamic balance between user privacy protection and normal app functionality. In China, national laws and regulations such as ''Personal Information Protection Law'' and ''Data Security Law'', and industry and group standard norms such as ''App User Rights Protection Measurement Norms'' and ''Minimum Necessary Assessment Norms for the Collection and Use of Personal Information by App'' have been introduced one after another, which to a certain extent provide guidance for the enforcement actions of regulatory authorities [19]. In April 2021, China's Ministry of Industry and Information Technology issued ''Interim Provisions on the Management of Personal Information Protection of Mobile Internet Applications'', which further clarified the basic principles of app personal information handling activities and the responsibilities and obligations of relevant subjects. But from the existing supervisory practice effect, a single, fragmented supervisory model is costly and inefficient. In fact, the app involves many ~~and~~ complex interest subjects, so it is difficult to effectively improve the app's personal information security issues just rely on the government. The multi-party collaboration and information sharing of app personal information security supervision is increasingly highlighting its superiority and becoming a trend [16], [21], [22]. In November 2021, the Ministry of Industry and Information Technology of China released the ''Fourteenth Five-Year Plan for the development of information and communication industry'' [23], which pointed out that a comprehensive supervision pattern with government supervision as the main focus should be built, and multiple parties should be fully absorbed to jointly participate in the governance of app personal information security.

In conclusion, in today's rapid development of the mobile Internet economy, the problem of personal information security of apps has gradually become the focus of public attention, and the study of multiple collaborative supervision modes plays a key role in optimizing the shortcomings of traditional supervision mode, and has important practical significance for protecting users' personal information security. At present, the China Academy of Information and Communication Research has organized the construction of a national app technical testing platform jointly with some Internet enterprises. Now it has built a complaint platform for Internet information services, and a number of user rights channels such as the Internet Association of China's Network Bad and Spam Information Reporting Center, which provides good conditions for information sharing and supervision under a collaborative perspective. Therefore, this paper will study the strategic behaviors of the main interest subjects of app personal information security supervision with the evolutionary game theory from the perspective of multi-party collaborative supervision. Theoretically, it can provide ideas for China and even other countries on the efficiency of app personal information security supervision.

The rest of the paper is structured as follows: Section II reviews the relevant research literature on app personal information security and evolutionary game theory. Section III constructs a tripartite evolutionary game model and payoff matrix for the collaborative supervision of local governments, app distribution platforms, and users, and analyzes the conditions for the existence of stable points of tripartite evolution of the game with the help of Lyapunov's first law. Section IV presents a numerical study to test the theoretical results and reveal the mechanisms by which key parameters affect the game process. Finally, Section V presents the main findings, limitations of the study, and future research directions.

II. LITERATURE REVIEW

In recent years, the problem of app personal information security has not only attracted wide attention from government departments and the public, but also become a research hotspot for many scholars. Academics have mainly conducted in-depth researches on the causes of app personal information security, the multi-party participation behavior in app personal information security, and the supervision of app personal information security under the evolutionary game.

A. THE CAUSES OF APP PERSONAL INFORMATION SECURITY

Scholars mainly analyze the causes of app personal information security problems from the perspectives of information asymmetry and user demand drive, among which user

demand is one of the main driving factors [24], [25], [26], [27], but the root cause is the existence of serious information asymmetry between app operators and users. The virtual, indirect and hidden characteristics of the app can easily cause information asymmetry, and app operators can take advantage of their information to collect and use users' personal information to gain profits by adopting illegal methods such as compulsory authorization, over-limit claiming, and excessive use [19]. Factors that contribute to information asymmetry also include inadequate vetting mechanisms, distorted information delivery, and restricted access. In terms of auditing mechanisms, Wang and Xu [28] pointed out that a large number of users have installed and used apps from unknown sources, and these apps make users' mobile terminals and personal information more vulnerable to attacks due to the lack of an authoritative auditing body. Yang [29] argued that the main reason why users are unsure whether the use of personal information is compliant is that app operators are not responsible for mandatory information disclosure for information flow and transfer, and most apps will require users to add access and even save permissions for their address book and SMS information, but users may not know whether this information is accessed, saved and used in large quantities. In terms of information delivery, Parker *et al.* [21] suggested that available information about data sharing may be subject to legal or technological constraints, which makes it difficult for the public to obtain appropriate information before deciding to use an app. Nurgalieva *et al.* [30] argued that despite the growing attention to privacy issues and regulations, relevant laws continue to be violated because users and regulators lack the tools to know when this is happening. Yoo *et al.* [31] pointed out that although some smartphone users are aware of the vulnerability of smartphones to cyber attacks, users are unaware of this due to the lack of information about security risks. In terms of access rights, Coleti *et al.* [32] mentioned that users often do not have access to or are unable to learn detailed information about the use of personal data, which raises concerns about privacy and security.

B. MULTI-PARTY PARTICIPATION BEHAVIOR IN APP PERSONAL INFORMATION SECURITY

Despite the high concern of users, enterprises and governments about the problem of app personal information security [33], the willingness of each subject to participate in supervision are generally low, which brings a big obstacle to the improvement of the efficiency of collaborative supervision. For the government, the government's avoidance behavior is the main reason [34]. On the one hand, the government lacks initiative and proactiveness, and in most cases, passive enforcement activities are launched only when major information security incidents that trigger widespread social concern break out [22]. On the other hand, the continuous expansion of app application fields has brought great pressure on the government's supervision. For example, the collection, storage, transmission, and ownership of personal information in health and fitness apps, which have developed rapidly in recent years, are almost unsupervised [35], [36]. For the app distribution platforms, compared to the government's inaction, the greater profit drive is more likely to prompt speculative behavior and continuously lower the market access threshold for apps [37], especially the lack of strict review of malware [31]. At the same time, it also encourages the speculative behavior of app operators [12]. Most of the users, who are the sources of information, have little interest or lack of security knowledge about personal information security problems [38]. Users' privacy burnout behaviors [39], [40], [41], privacy paradox behaviors [42], [43], etc. can affect their interest. Wang and Xu [28] pointed out that most users do not check and update the app frequently due to a lack of security habits. Currently, the emergence of app privacy policies has narrowed the information gap between app operators and users to a certain extent, but this approach fails to address the root of the problem. O'Loughlin *et al.* [44] found that most apps are still not transparent enough in terms of data security information after reviewing app privacy policies. Not only that, apps usually use formatted bullying clauses to force users to authorize the app to obtain relevant personal information, and if users choose not to authorize it, then they will directly not be allowed to use it [12]. Under such strong rules, most users tend not to read the privacy policies carefully considering the time cost, and thus tolerate such violations [45], [46], [47]. Therefore, how to effectively mobilize the participation of multiple parties in supervision has become an important research content.

C. THE SUPERVISION OF APP PERSONAL INFORMATION SECURITY UNDER THE EVOLUTIONARY GAME

Evolutionary game theory [48], [49] takes a finite rational game as the analytical framework, and the game parties achieve dynamic equilibrium through the process of continuous learning and adaptation, which makes up for the defects of traditional game theory such as assuming the participants are perfectly rational and have complete information. In the process of the evolutionary game, individuals often dynamically adjust their own strategies based on observing and learning other individuals' strategies. Evolutionary game theory has now been widely used in various types of supervision, such as environmental protection [50], [51], drug quality [52], information disclosure [53], and information security [54], and many scholars have extended the game subjects to three or even four to optimize the game model. On the use of evolutionary game theory to study the supervision of app personal information security, Zhu *et al.* [55] constructed an evolutionary game model of patients and medical app service providers considering government participation, and pointed out that the privacy strategies of patients and app service providers are closely related to their accountability costs, compensation amounts, supervisory efforts and privacy losses. Zhou and Qian [56] constructed a two-sided game model between apps that over-collect information and the governments, and the strategy choices of both sides of the game are closely related to the cost of personal data

protection, the probability of data leakage, government supervisory penalties and the cost of supervision. Qu and Hou [57] considered the counteracting behaviors of platforms to users' rights, and constructed a three-party game model of platforms, users and governments.

In summary, the existing research provides a theoretical and practical basis for the supervision of app personal information security. Although this has some reference value, there are still shortcomings: (1) Although scholars have explored the causes of the current situation of app personal information security supervision and the supervisory role of the main responsible subjects, few studies have taken users' feedback into account, and more often analyzed users' willingness to use an app from the perspective of privacy protection. In fact, in the current information environment, the value of information brought by users' feedback is very beneficial to the supervision. (2) The participation behaviors of different subjects in personal information security problems are analyzed, but the phenomena of confrontation and cooperation among subjects are less explained from the perspective of a dynamical system. In fact, app operators will form a long-term game relationship with their game opponents (such as users, peers, upstream and downstream enterprises, supervisors, etc.) over a longer period of time because of the organizational characteristics of enterprise nature. The evolutionary game theory has been adopted to explore the supervision of app personal information security, but there is a lack of research on multi-party participation in supervision from the perspective of information sharing and cooperation and collaboration. Thus, it can be seen that considering the feedback mechanism of users and establishing a collaborative supervisory mechanism of app personal information security with multi-party participation plays an important role in making up for the shortcomings of the traditional supervisory model. The main contributions of this paper are as follows: (1) How does users' feedback affect the strategy choices of local governments, APP distribution platforms and users? (2) In response to the impact of changes in key parameters on the evolutionary stabilization strategies of each game subject, how should the government take supervisory measures and coordinate the interests of each subject so as to effectively curb the consequences of the app personal information security problem?

III. EVOLUTIONARY GAME MODEL

A. PROBLEM DESCRIPTION

Compared with the traditional offline service mode, app achieves higher service quality accessibility with the help of personal information, but it is difficult to achieve effective management just by government supervision because of more interest subjects involved. Therefore, the construction of multi-party participation, information sharing app personal information security supervision mode, not only can ease the pressure of government supervision, but also can mobilize social forces, play a synergistic effect, and better maintain the market order.

By combing the basic vein of app operation, we can get app personal information security multi-party collaborative supervision mode is mainly divided into three levels: First, administrative supervision from relevant government departments. In China, the central government urges local governments to implement the supervision of app-related operation organizations within their own administrative jurisdictions, and third-party testing organizations obtain the authorization of government departments to conduct testing and evaluation of app operators, and then deliver information such as app personal information security review results to government departments and publish them on the supervisory information platform. Second, self-supervision from app's related industry organizations. App-related operation organizations regulate the behavior of app distribution platforms and app operators through relevant industry standards. App distribution platforms should take regular review work for app operators and disclose the review results in a timely manner. App operators should report their operations to app distribution platforms regularly in addition to self-regulation. Third, the supervision from user rights. Users should actively participate in the supervision work, give positive feedback to apps with high security coefficients, and provide timely complaint feedback to the supervisory information platform for apps with bad operation [58]. Therefore, the structure relationship of app personal information security supervision constructed in this paper is shown in Figure 1.

B. MODEL ASSUMPTIONS

Based on the problem description, we select the players that play a larger role in the multi-party collaborative supervision of app personal information security for game analysis. It is assumed that there are three game players, who are local governments, app distribution platforms and users, and they are all finite rational. In the beginning, their strategy is not optimal. They learn, experiment, and adjust until they reach an equilibrium. Local governments have two alternative strategies, either to actively implement the central government's requirements to supervise the personal information security practices of app operators, or not to supervise against the central government's requirements. The space of strategic choices for local governments is {supervise G_1, unsupervised G_2}. App distribution platforms have two strategic choices, one is to review apps according to legal requirements and industry standards, and the other is not to review apps for violations against the requirements. The space of strategic choices for app distribution platforms is {review P_1, unreviewed P_2}. Users also have two strategic choices, either to evaluate and give feedback on the app's behavior or to choose to do nothing at all. The space of strategic choices for users is {feedback U_1, no feedback U_2}. The basic assumptions are as follows.

Assumption 1: The probability that the local government chooses the 'supervise G_1' strategy is x, $x \in [0, 1]$, and the probability that the 'unsupervised G_2' strategy is $1 - x$. The probability that the app distribution platform chooses the

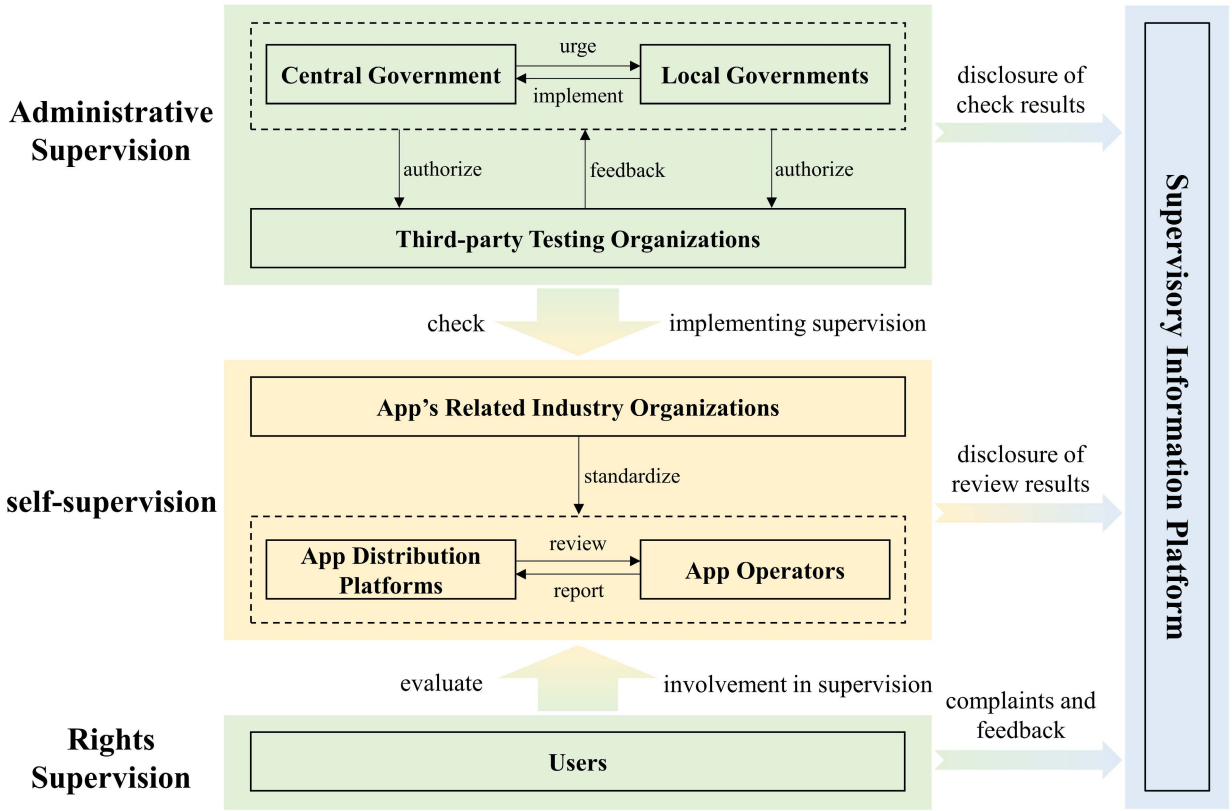

FIGURE 1. App personal information security multi-party collaborative supervision structure relationship diagram.

'review P_1' strategy is y, $y \in [0,1]$, and the probability that the 'unreviewed P_2' strategy is $1-y$. The probability that the user chooses the 'feedback U_1' strategy is z, $z \in [0, 1]$, and the probability that the 'no feedback U_2' strategy is $1-z$.

Assumption 2: When the local government chooses the supervise strategy, its supervisory cost is C_g. When the app has personal information security problems, the penalty that the app distribution platform will receive when it adopts the unreviewed strategy is F_p. The review cost of the app distribution platform is C_p and the feedback cost of the user is C_u. The violation probability of the app operator is γ.

Based on the above basic assumptions, the main scenarios we can obtain are as follows.

Scenario 1: Local government chooses supervise strategy, app distribution platform chooses review strategy, and user chooses feedback strategy. When the local government releases information such as app personal information security testing results in the supervisory information platform, the value of information obtained by user at this time is V_g. When the local government and the app distribution platform publish information at the same time, the value of information obtained by the user is V. At this time, the user will receive a synergistic information premium. This is because the information obtained by the user from both parties at the same time can improve the authenticity of the information, so $V > V_g$ and $V > V_p$. For local government and app distribution platform, the joint role of both in the regulation of APP personal information security generates synergistic effects. Drawing on previous studies [59], the Cobb-Douglas production function in economics can be used to reflect the benefits of both, which is $\mu I_g^{\alpha} I_p^{\beta}$ (where I_g and I_p are the supervisory inputs of local government and app distribution platform respectively, μ is the coefficient of synergy effect, α and β are the coefficients of information transfer efficiency in the collaborative supervision of local government and app distribution platform respectively). Then the synergistic benefits obtained by the local government and the app distribution platform are $\varphi\mu I_g^{\alpha} I_p^{\beta}$, $(1-\varphi)\mu I_g^{\alpha} I_p^{\beta}$, where φ is the benefit distribution coefficient. When users use the app, they can give feedback through the supervisory information platform, i.e., this information is fed back to the supervisory information platform and make positive comments. The resulting reputation value premiums to local governments and app distribution platforms are R_g and R_p.

Scenario 2: Local government chooses supervise strategy, app distribution platform chooses review strategy, and user chooses no feedback strategy. At this time, local government and app distribution platform will not get reputation value premium.

Scenario 3: Local government chooses supervise strategy, app distribution platform chooses unreviewed strategy, and user chooses feedback strategy. At this time, the local

government finds that app has personal information security problems, then the app distribution platform will be punished.

Scenario 4: Local government chooses supervise strategy, app distribution platform chooses unreviewed strategy, and user chooses no feedback strategy. Since local government is not mandatory for user's feedback behavior, user's non-feedback behaviors will not be punished by local government.

Scenario 5: Local government chooses unsupervised strategy, app distribution platform chooses review strategy, and user chooses feedback strategy. User will unilaterally get the information value from app distribution platform. In addition, due to the information asymmetry factor, user do not know whether the supervisory role of local government or the review behavior of app distribution platform takes effect, so both local government and app distribution platform will get the reputation value premium.

Scenario 6: Local government chooses unsupervised strategy, app distribution platform chooses review strategy, and user chooses no feedback strategy. Neither the local government nor the app distribution platform will receive the reputation value premium.

Scenario 7: Local government chooses unsupervised strategy, app distribution platform chooses unreviewed strategy, and user chooses feedback strategy. The local government will suffer the administrative punishment of the central government as F_g. When the app has personal information security problems, the user will suffer the loss as L_u. At this time, the user can choose to give feedback to the supervisory information platform, make negative comments on the app distribution platform and make complaints to defend the rights, the central government will urge the local government and app distribution platform to give compensation to the user, the user can get the compensation of the app operator as B_u. Local government and APP distribution platform will suffer reputation loss as L_g and L_p, while app distribution platform will also be additionally punished.

Scenario 8: Local government chooses unsupervised strategy, app distribution platform chooses unreviewed strategy, and user chooses no feedback strategy. User will suffer loss, local government and app distribution platform will not gain or lose.

The details of the three-party game matrix of local governments, app distribution platform and user are shown in Table 1.

C. REPLICATION DYNAMIC EQUATION

Based on the above basic assumptions and Table 1, we can obtain the expected returns and the average expected returns of local government, app distribution platform and user choosing positive and negative strategy as shown below.

$$\begin{aligned}
U_{G_1} &= (1-\gamma+\gamma y)\,R_g z+\gamma F_p-C_g \\
&\quad +\left(\varphi\mu I_g^{\alpha} I_p^{\beta}-\gamma F_p\right) y && (1)\\
U_{G_2} &= R_g yz-(F_g+L_g)(1-y)z && (2)\\
\overline{U}_G &= xU_{G_1}+(1-x)U_{G_2} && (3)\\
U_{P_1} &= R_p z-C_p+(1-\varphi)\,\mu I_g^{\alpha} I_p^{\beta} x && (4)\\
U_{P_2} &= ((\gamma(F_p+L_p-R_p)+R_p)z)-\gamma F_p)x \\
&\quad -\gamma(F_p+L_p)z && (5)\\
\overline{U}_P &= yU_{P_1}+(1-y)\,U_{P_2} && (6)\\
U_{U_1} &= (V_p+\gamma(L_u-B_u)\text{-}(V_g-V+V_p \\
&\quad +\gamma(L_u-B_u))x)y+(V_g+\gamma(L_u-B_u))x-C_u \\
&\quad +\gamma(B_u-L_u) && (7)\\
U_{U_2} &= ((V-V_g)x-(1-x)(V_p+\gamma L_u))y \\
&\quad +(V_g+\gamma L_u)x-\gamma L_u && (8)\\
\overline{U}_U &= zU_{U_1}+(1-z)U_{U_2} && (9)
\end{aligned}$$

According to the Malthusian equation, the replication dynamic equation of the three players can be obtained, i.e.

$$F(x)=\frac{dx}{dt}=x\left(U_{G_1}-\overline{U}_G\right)=x(1-x)\left(U_{G_1}-U_{G_2}\right) \tag{10}$$

$$F(y)=\frac{dy}{dt}=y\left(U_{P_1}-\overline{U}_P\right)=y(1-y)\left(U_{P_1}-U_{P_2}\right) \tag{11}$$

$$F(z)=\frac{dz}{dt}=z\left(U_{U_1}-\overline{U}_U\right)=z(1-z)\left(U_{U_1}-U_{U_2}\right) \tag{12}$$

D. EQUILIBRIUM POINT AND STABILITY ANALYSIS

From (10), (11) and (12), the three-dimensional dynamical system (S) consisting of replicated dynamic equations for the three game players is (13), as shown at the bottom of the page.

From (13), the Jacobian matrix of the system (S) is given as follows.

$$J\begin{bmatrix}
\partial F(x)/\partial x & \partial F(x)/\partial y & \partial F(x)/\partial z \\
\partial F(y)/\partial x & \partial F(y)/\partial y & \partial F(y)/\partial z \\
\partial F(z)/\partial x & \partial F(z)/\partial y & \partial F(z)/\partial z
\end{bmatrix}$$

In a multi-party evolutionary game, if the equilibrium solution of the game is an evolutionary steady state, the equilibrium is a strict Nash equilibrium, which can also be called a pure strategic equilibrium. Therefore, we only need to analyze the asymptotic stability of the eight pure strategy equilibria in the system (S). Let $F(x)=F(y)=F(z)=0$, we can get 8 pure strategy equilibria, which are $E_1(0,0,0)$, $E_2(0,0,1)$, $E_3(0,1,0)$, $E_4(0,1,1)$, $E_5(1,0,0)$,

$$\begin{cases}
F(x)=x(1-x)((R_g+\boldsymbol{\gamma}(F_g+L_g-R_g)+\boldsymbol{\gamma}(R_g-F_g-L_g)y)z+\boldsymbol{\gamma}F_p-C_g+(\varphi\mu I_g^{\alpha}I_p^{\beta}-\boldsymbol{\gamma}F_p)y) \\
F(y)=y(1-y)((R_p+\boldsymbol{\gamma}(F_p+L_p)+(\boldsymbol{\gamma}(R_p-F_p-L_p)-R_p)x)z-C_p+(\boldsymbol{\gamma}F_p-\varphi\mu I_g^{\alpha}I_p^{\beta})x) \\
F(z)=z(1-z)(\gamma(1-x)(1-y)B_u-C_u)
\end{cases} \tag{13}$$

TABLE 1. The three-party game matrix of local government, APP distribution platform and user.

Strategy Combinations	Local Government	App Distribution Platform	User
$(G_1,\ P_1,\ U_1)$	$R_g+\varphi\mu I_g^{\alpha}I_p^{\beta}-C_g$	$R_p+(1-\varphi)\mu I_g^{\alpha}I_p^{\beta}-C_p$	$V-C_u$
$(G_1,\ P_1,\ U_2)$	$\varphi\mu I_g^{\alpha}I_p^{\beta}-C_g$	$(1-\varphi)\mu I_g^{\alpha}I_p^{\beta}-C_p$	V
$(G_1,\ P_2,\ U_1)$	$(1-\gamma)R_g-C_g+\gamma F_p$	$(1-\gamma)R_p-\gamma F_p$	V_g-C_u
$(G_1,\ P_2,\ U_2)$	$-C_g+\gamma F_p$	$-\gamma F_p$	V_g
$(G_2,\ P_1,\ U_1)$	R_g	$-C_p+R_p$	V_p-C_u
$(G_2,\ P_1,\ U_2)$	0	$-C_p$	V_p
$(G_2,\ P_2,\ U_1)$	$-\gamma F_g-\gamma L_g$	$-\gamma L_p-\gamma F_p$	$\gamma B_u-\gamma L_u-C_u$
$(G_2,\ P_2,\ U_2)$	0	0	$-\gamma L_u$

$E_6(1,0,1)$, $E_7(1,1,0)$ and $E_8(1,1,1)$. According to Lyapunov's first law, if all the eigenvalues of the Jacobian matrix are negative, the equilibrium is an evolutionary stability point (ESS). If the Jacobian matrix has at least one positive eigenvalue, then the equilibrium is an unstable point. If the Jacobian matrix has all negative eigenvalues except zero, then the equilibrium point is indeterminate in terms of stability. Let λ_1, λ_2 and λ_3 be the three eigenvalues of the system (S). The eigenvalues of the corresponding Jacobian matrix can be obtained by substituting the eight pure policy equilibrium points of the system into the Jacobian matrix. The details are shown in Table 2.

From Table 2, the possible evolutionary stability points of system (S) are $E_1(0,0,0)$, $E_2(0,0,1)$, $E_5(1,0,0)$ and $E_7(1,1,0)$, i.e., {unsupervised, unreviewed, no feedback}, {unsupervised, unreviewed, feedback}, {supervise, unreviewed, no feedback}, {supervise, review, no feedback}. We next discuss the stability conditions for the possible evolutionary stability points.

Assignment a: When the two conditions $\gamma F_p - C_g < 0$ and $\gamma B_u - C_u < 0$ are satisfied, (0,0,0) is ESS.

Assignment b: When the three conditions $\gamma(F_g+L_g-R_g+F_p)+R_g-C_g<0$, $R_p+\gamma(L_p+F_p)-C_p<0$ and $-(\gamma B_u-C_u)<0$ are satisfied, (0,0,1) is ESS.

Assignment c: When the two conditions $-(\gamma F_p - C_g) < 0$ and $-C_p-\varphi\mu I_g^{\alpha}I_p^{\beta}+\gamma F_p<0$ are satisfied, (1,0,0) is ESS.

Assignment d: When the two conditions $-(-C_g+\varphi\mu I_g^{\alpha}I_p^{\beta})<0$ and $-(-C_g+\varphi\mu I_g^{\alpha}I_p^{\beta})<0$ are satisfied, (1,1,0) is ESS.

The four scenarios allow us to make the following guesses.

Guess 1: In practice, *assignment b* is better relative to *assignment a*. Therefore, in order to avoid (0,0,0) from becoming ESS, we can take the following measures. The equilibrium of the game can be induced to shift from *assignment a* to *assignment b* by increasing the penalty imposed by local government on app distribution platform, reducing the cost of supervision by local government and the cost of feedback from user.

Guess 2: Assignment d is better compared to *assignment a*, *assignment b*, and *assignment c*. Therefore, in order to make (1,1,0) become ESS, we can take the following steps are. Increase the penalty of central government to local government, increase the penalty of local government to app distribution platform, increase the reputation value premium and reputation loss from user feedback to local government and app distribution platform, reduce the cost of supervision by local government and reduce the cost of review by app distribution platform. At the same time, it can also increase the synergy gain. The above practices can drive the game equilibrium from *assignment a*, *assignment b* and *assignment c* to *assignment d*.

IV. NUMERICAL SIMULATIONS

Based on the development status and statistics of apps operating in China at the present stage, we propose a numerical study to simulate the behavior of game players, which can theoretically provide reference values for the supervision of app personal information security problems in a global context.

A. SETTING INITIAL VALUES

Currently there is still a lack of complete statistical data on the supervision of app personal information security. In order to ensure the availability and authenticity of the simulated data as much as possible, we use the existing relevant data to set some of the parameter values, and the data for this part of the initial parameters are mainly from industry analysis reports, national standards and government websites of the central government, provinces and cities, etc. Other parameter values are set based on relevant literature, enterprises and experts in the relevant fields, global data or practical data from other countries, etc.

Apps operating in China are jointly supervised by the Office of Network Security and Information Technology Commission, the Ministry of Industry and Information Technology, the Ministry of Public Security, and the State Administration of Market Supervision and Administration. A review of each department's annual budget statement for 2021 shows that general public service expenditures and information industry supervisory expenditures, which are

TABLE 2. Stability analysis of replicated dynamic system(s).

Equilibrium points	eigenvalues			Positive and negative sign	Stability
	λ_1	λ_2	λ_3		
$E_1(0,0,0)$	$\gamma F_p - C_g$	$-C_p$	$\gamma B_u - C_u$	$(\pm,-,\pm)$	Uncertain
$E_2(0,0,1)$	$\gamma(F_g + L_g - R_g + F_p) + R_g - C_g$	$R_p + \gamma(L_p + F_p) - C_p$	$-(\gamma B_u - C_u)$	$(\pm,\pm,\pm)$	Uncertain
$E_3(0,1,0)$	$-C_g + \varphi\mu I_g^\alpha I_p^\beta$	C_p	$-C_u$	$(\pm,+,-)$	Not ESS
$E_4(0,1,1)$	$(1-\gamma)(R_g - F_p - L_g) + R_g - C_g + \varphi\mu I_g^\alpha I_p^\beta$	$-(R_p + \gamma(F_p + L_p) - C_p)$	C_u	$(\pm,\pm,+)$	Not ESS
$E_5(1,0,0)$	$-(\gamma F_p - C_g)$	$-C_p - \varphi\mu I_g^\alpha I_p^\beta + \gamma F_p$	$-C_u$	$(\pm,\pm,-)$	Uncertain
$E_6(1,0,1)$	$-(\gamma(F_g + L_g - R_g + F_p) + R_g - C_g)$	$\gamma(2F_p + L_p + R_p) - F_p - L_p - C_p - \varphi\mu I_g^\alpha I_p^\beta$	C_u	$(\pm,\pm,+)$	Not ESS
$E_7(1,1,0)$	$-(-C_g + \varphi\mu I_g^\alpha I_p^\beta)$	$-(-C_p + \gamma F_p - \varphi\mu I_g^\alpha I_p^\beta)$	$-C_u$	$(\pm,\pm,-)$	Uncertain
$E_8(1,1,1)$	$-((1-\gamma)(R_g - F_p - L_g) + R_g - C_g + \varphi\mu I_g^\alpha I_p^\beta)$	$-\gamma(2F_p + L_p + R_p) + F_p + L_p + C_p + \varphi\mu I_g^\alpha I_p^\beta$	C_u	$(\pm,\pm,+)$	Not ESS

strongly related to security and supervisory affairs, total about 19.642 billion yuan. The report '2022 China Mobile Economy Development' states that the mobile economy accounts for 5.6% of China's GDP. Therefore, the initial value of supervisory cost for local government is set as 11. According to the 'Research Report on the Information Security Status of Chinese Internet Users in 2021', the total amount of personal losses brought about by information security incidents is about 20 billion yuan, and the accumulated recovered losses are 4.12 billion yuan, of which 5% originate from app. so the initial value of user losses is set to 10. The initial value of user compensation is 2.06. In 2021, Beijing Communication Authority tested 43 app distribution platforms in the administrative jurisdiction and interviewed 13 non-compliant platforms according to the law. Therefore, set the initial policy selection probability of app distribution platforms as 0.3. In December 2021, the National Computer Network Emergency Technology Processing Coordination Center released the 'App Illegal and Illegal Collection and Use of Personal Information Monitoring and Analysis Report', which launched a test on 1,425 apps heavily used by the public, of which 351 had serious problems of excessive collection of personal information. Therefore, the probability of app violation is set at 0.25.

The other values are assigned according to the previous setting basis. The initial values of all parameters are shown in Table 3.

B. SIMULATION RESULTS AND DISCUSSION

MatlabR2021a software is used for evolutionary game model simulation. The evolutionary stability of the system (S) with the initial value is shown in Figure 2. The equilibrium point of the system (S) at this time is (0,0,0), i.e. {unsupervised, unreviewed, no feedback}. This implies that the current state of practice is not theoretically optimal. Therefore, we construct five scenarios in the subsequent section to analyze the evolutionary stabilization strategies of the game players.

TABLE 3. Copy the initial value of the dynamic system(s).

Parameter	Value	Parameter	Value
x	0.5	R_g	8
y	0.3	R_p	6
z	0.5	F_g	20
C_g	11	F_p	20
C_p	15	γ	0.25
C_u	4	L_g	5
$\mu I_g^\alpha I_p^\beta$	30	L_p	5
φ	0.5	B_u	2.06

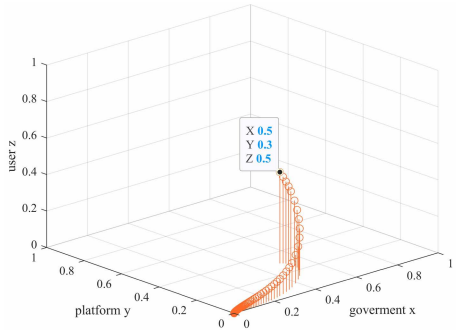

FIGURE 2. Three-dimensional evolutionary stability diagram of each game player under initial values.

1) THE IMPACT OF PENALTY ON GAME PLAYERS

To analyze the impact of F_p on the strategy choice of the game players, we set $F_p \in [0, 40]$ with a step size of 10, and the simulation results are shown in Figure 3. At initial values, i.e., when $F_p = 20$, the evolutionary stabilization strategies of both local government and app distribution platform are negative, i.e., {unsupervised, unreviewed}. When F_p decreases, the convergence rate of local government and app distribution platform choosing negative strategies becomes faster. As F_p gradually increases, the convergence rate of local government and app distribution platform evolving to negative strategies

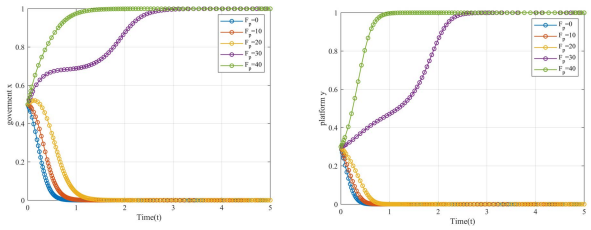

FIGURE 3. Impact of F_p changes on local government and app distribution platform.

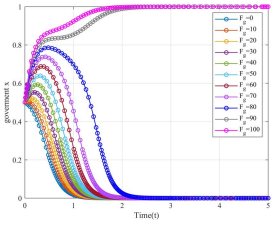

FIGURE 4. Impact of F_g changes on local government.

becomes significantly slower. As F_p continues to increase, the direction of the evolutionary stabilization strategy of local government and app distribution platform changes to a positive strategy, i.e., {supervise, review}. It can be obtained that when the penalty amount of local government on app distribution platform is increased, it can effectively promote the game players to adopt positive strategies. This verifies the conjecture in the previous guess.

To analyze the impact of F_g on local government strategy choice, we set $F_g \in [0, 100]$ with a step size of 10, and the simulation results are shown in Figure 4. Under the initial value, i.e., when $F_g = 20$, the evolutionary stabilization strategy of the local government is unsupervised. When F_g decreases, the convergence of local government choosing negative strategy becomes faster. When F_g increases, the convergence rate of local government evolution to negative strategy becomes progressively slower. When F_g increases to a certain level, the direction of the evolutionary stabilization strategy of the local government changes to a positive strategy. It can be obtained that the increase of penalty amount can effectively promote local government to adopt positive strategy, which verifies the previous guess.

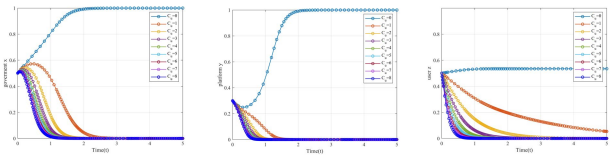

FIGURE 5. Impact of C_u changes on local government, app distribution platform and user.

2) THE IMPACT OF USER FEEDBACK COST ON GAME PLAYERS

To analyze the impact of C_u on the strategy choice of the game players, we set $C_u \in [0, 8]$ with a step size of 1, and the simulation results are shown in Figure 5. The increase in C_u promotes the choice of negative strategies by the three gaming players. This is because the probability of user feedback will gradually increase when the cost of user feedback decreases, and local government and app distribution platform gradually increase the probability of supervision and review in order to maintain their reputation and avoid punishment. Under the initial value, i.e., $C_u = 4$, the evolutionary stabilization strategies of all three players of the game are negative strategies as {unsupervised, unreviewed, no feedback}. When C_u decreases to 0, the direction of evolutionary stabilization strategy of local government and app distribution platform changes to positive strategy. The evolutionary stabilization strategy of the user does not converge to 1, but it remains stable with a high probability. Therefore, reducing the cost of user feedback can not only motivate user's feedback, but also promote the evolutionary stabilization strategy of local government and app distribution platforms to a positive strategy. This verifies the previous guess.

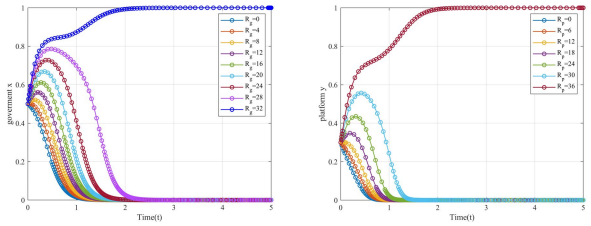

FIGURE 6. Impact of R_g changes on local government, Impact of R_p changes on app distribution platform.

3) THE IMPACT OF REPUTATION VALUE PREMIUM ON GAME PLAYERS

To analyze the impact of R_g on local government strategy choice, we set $R_g \in [0, 32]$ with a step size of 4. To analyze the impact of R_p on app distribution platform strategy choice, we set $R_p \in [0, 36]$ with a step size of 6. The simulation results are shown in Figure 6. When $R_g = 8$, the evolutionary stabilization strategy of the local government is a negative strategy. When R_g decreases, the convergence rate of local government choosing negative strategy becomes faster. As R_g increases, the convergence rate of local government evolution to negative strategy becomes progressively slower. When R_g increases to a certain level, the direction of the evolutionary stabilization strategy of the local government changes to a positive strategy. The impact of R_p on app distribution platform has the same trend as the impact of R_g on local government. It can be obtained that the reputation value premium is positively related to both local government and app distribution platform's choice of positive strategies. Therefore, when the reputation value premium from user feedback increases, it can effectively promote local government and app distribution platform to adopt positive strategies. This verifies the previous guess.

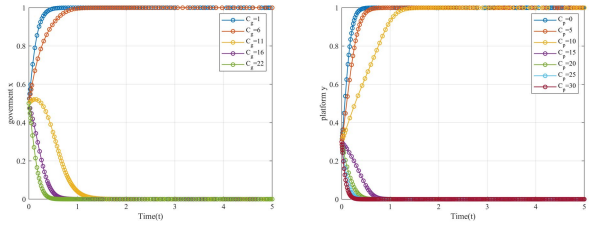

FIGURE 7. Impact of C_g changes on local government, Impact of C_P changes on app distribution platform.

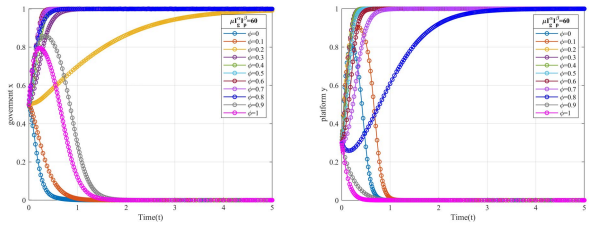

FIGURE 9. When $\mu I_g^{\alpha} I_P^{\beta} = 60$, the impact of φ change on local government and app distribution platform.

4) THE IMPACT OF SUPERVISORY AND REVIEW COSTS ON GAME PLAYERS

To analyze the impact of C_g on local government strategy choice, we set $C_g \in [1, 22]$ with a step size of 5. To analyze the impact of C_p on app distribution platform strategy choice, we set $C_p \in [0, 30]$ with a step size of 5. The simulation results are shown in Figure 7. When $C_g = 11$, the evolutionary stabilization strategy of the local government is a negative strategy. When C_g increases, the convergence rate of local government choosing negative strategy becomes faster. As C_g decreases, the convergence rate of local government evolution to negative strategy becomes progressively slower. When C_g decreases to a certain level, the direction of the evolutionary stabilization strategy of the local government changes to a positive strategy. The impact of C_p on app distribution platform has the same trend as the impact of C_g on local government. It can be obtained that the cost of supervision is negatively related to the choice of positive strategy by local government, and the cost of review is negatively related to the choice of active strategy by app distribution platform. Therefore, when the cost of supervision and review is reduced, it can effectively facilitate local government and app distribution platform to adopt positive strategies. This verifies the previous guess.

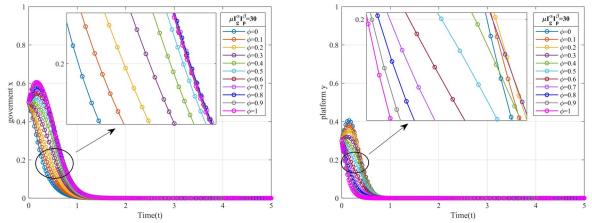

FIGURE 8. When $\mu I_g^{\alpha} I_P^{\beta} = 30$, the impact of φ change on local government and app distribution platform.

5) THE IMPACT OF SYNERGISTIC BENEFITS ON GAME PLAYERS

To analyze the impact of φ on the strategy choice of the game players, we set $\varphi \in [0, 1]$ with a step size of 0.1, and the simulation results are shown in Figure 8. When φ decreases, the convergence speed of local government choosing negative strategy becomes faster, while the convergence speed of app distribution platform choosing negative strategy becomes slower. As φ increases, the convergence speed of local government choosing negative strategy becomes slower, while the convergence speed of app distribution platform evolving to negative strategy gradually becomes faster. However, regardless of the value of φ, the evolutionary stabilization strategy of both local government and app distribution platform is negative, i.e., {unsupervised, unreviewed}. It can be obtained that φ is positively related to the choice of active strategy by local government and negatively related to the choice of active strategy by app distribution platform.

To analyze the impact of $\mu I_g^{\alpha} I_p^{\beta}$ on the strategy choice of the game players, we set $\mu I_g^{\alpha} I_p^{\beta} = 60$, and the simulation results are shown in Figure 9. When $\varphi \in [0.2, 0.8]$, the evolutionary stabilization strategy of local government and app distribution platform is positive. When $\varphi = 0$,0.1,0.9 and 1, the evolutionary stabilization strategy of local government and app distribution platform is negative. By comparing Figure 7 and Figure 8, it can be found that local government and app distribution platform start to appear to evolve towards a positive strategy when the $\mu I_g^{\alpha} I_p^{\beta}$ increase. It can be obtained that the synergistic benefit is positively related to the choice of positive strategies by both local government and app distribution platform. Therefore, when the synergistic benefit is increased, it can effectively promote local government and app distribution platform to adopt positive strategies. This verifies the previous guess. In addition, when φ is more homogeneous, the more it helps local government and app distribution platform to evolve stable strategies to positive strategies.

C. ANALYSIS OF RESULTS

Based on the simulation results, it is clear that the following measures can promote proactive strategies for local government and app distribution platform. (1) Increase the penalty for local government and app distribution platform, increase the premium of reputation value or reputation loss from user feedback, and increase the synergistic benefit. (2) Reducing the cost of supervision for local government can promote it to adopt positive strategy, and reducing the cost of review for app distribution platform can promote it to adopt positive strategy. (3) Reducing the cost of user feedback can not only improve user's enthusiasm to participate in supervision, but also promote local government and app distribution platform to adopt positive strategies. (4) When the synergistic benefits

are more evenly distributed, it is more favorable for local government and app distribution platform to adopt positive strategies.

Combined with the simulation results, this paper proposes the following three optimization strategies for the problem of collaborative supervision of app personal information security.

(1) Reduce the cost of participation in collaborative supervision by all parties involved in the game. The cost for local government, app distribution platform and user to participate in supervision is an important influencing factor in their strategy choice. For app distribution platform, it is necessary to reduce the cost of review by building an effective security review system, optimizing the review process and so on. For local government, first of all, higher-level departments can try to increase subsidies and mobilize local governments to actively participate in supervisory initiatives. Secondly, government can introduce blockchain and other supervisory technologies to improve regulatory efficiency, which can effectively reduce supervisory costs. Finally, the cost of user feedback should be reduced. Reduce the cost of user feedback can not only improve the enthusiasm of user feedback, but also enable government to receive feedback from users in a timely manner and truly achieve compliance with the law. Therefore, information sharing and interoperability should be achieved by improving and promoting online complaint platforms and online arbitration mechanisms. This helps to promote users to adopt positive feedback strategies and is important to alleviate the problem of app personal information security.

(2) Increase the reputational value premium or reputation loss brought by user feedback to local government and app distribution platform, and increase the penalty for their negative behavior. The government should improve the user feedback mechanism through smooth feedback channels, guide users to enhance their awareness of their rights, and encourage them to make a true and objective evaluation of the app's personal information handling behavior in the supervisory information platform. When users find that the app has irregularities, they should actively complain or report to the government, and such behavior is conducive to the government's additional punishment of the responsible subject. The greater the penalty for unreviewed of app distribution platforms, the more platforms will not dare to take the risk. They will cooperate with government in censoring apps with higher probability, and nip the problem of personal information security at an early stage. Higher-level departments should also increase the administrative penalty on local government. Local government should be urged to actively implement good supervision and timely report the review results to the supervisory information platform, which is conducive to timely access to information by the community. In addition, local government can try to take positive incentives in the form of reputation rewards for app distribution platform. The influence of social opinion can promote the platform to adopt positive behavior, which is more applicable in many industries.

(3) Increase and rationalize the distribution of synergistic benefit. The improved synergistic benefit will prompt local government and app distribution platform to choose positive strategies. First, local government can borrow the government information work assessment mechanism to establish the app distribution platform security review information assessment mechanism. Second, to regularly inform the app distribution platform information reporting and uploading work. Finally, the credibility points of app distribution platform should be recorded, which can motivate app distribution platform to share app information and personal information usage on the supervisory information platform. In addition, the synergistic benefit should be reasonably distributed. When the synergistic benefit is distributed more evenly, the highest efficiency of synergistic benefit distribution between local government and app distribution platform can be achieved. This is conducive to a win-win situation of cooperation between the two sides.

V. CONCLUSION

Strengthening the supervision of app personal information security can effectively promote the healthy development of mobile Internet economy. The government, app-related industry organizations and academia are currently studying how to coordinate the resources of all parties to participate in the supervision in a coordinated manner. Most of the previous studies have explored the effectiveness of supervision from the perspective of the main regulatory bodies, and have not been able to reveal the changes in the strategic choices of each body on the issue of app personal information security supervision under the feedback mechanism of user participation. To this end, this paper firstly establishes a three-party cooperative supervisory evolutionary game model of local government, app distribution platform and user. Secondly, the possible stability points and their stability conditions are analyzed. Finally, we analyze the evolutionary stabilization strategies of the three game players with the help of case data from China, and discuss the influence of changes in key parameters on the evolutionary stabilization strategies of the game players. The results show that supervisory efficiency can be improved in three ways. Reducing the cost of participation in collaborative supervision for all game players, increasing the punishment for game players with primary supervisory responsibility, and increasing and reasonably distributing the benefits of collaboration.

At the theoretical level, this paper explores the applicability of evolutionary game theory to the problem of app personal information security supervision, providing a new perspective for current research in related fields. At the practical level, by constructing a three-party evolutionary game model of cooperative supervision among local governments, app distribution platforms and users, we find the important influencing factors that can help improve the efficiency of cooperative supervision and put forward feasible strategic

suggestions. At the same time, there are still shortcomings in this paper. Firstly, in the process of app personal information security supervision, the main interest party app operators are not taken into account. Secondly, among the possible stable points, due to the limitation of parameter setting, there is no condition that makes all game players adopt positive strategies. Therefore, the future research can be expanded in the following two aspects. First, by constructing a four-party evolutionary game model, and we will analyze the supervision mechanism of app personal information security in which local governments, app distribution platforms, app operators and users participate together. Second, we will consider giving positive incentives to the players involved in the supervision, which may promote the existence of stable points where all parties adopt positive strategies.

REFERENCES

[1] C. Xue, W. Tian, and X. Zhao, "The literature review of platform economy," *Sci. Program.*, vol. 2020, pp. 1–7, Sep. 2020.
[2] S. Hong, C. Liu, B. Cheng, B. Ren, and J. Chen, "MobiGemini: Sensitive-based data and resource protection framework for mobile device," *China Commun.*, vol. 14, no. 7, pp. 1–11, Jul. 2017.
[3] H. Chen, S. Lee, and D. Jeong, "Application of a FL time series building model in mobile network interaction anomaly detection in the Internet of Things environment," *Comput. Intell. Neurosci.*, vol. 2022, pp. 1–8, Feb. 2022.
[4] J. Chen, B. Li, J. Wang, Y. Zhao, L. Yao, and Y. Xiong, "Knowledge graph enhanced third-party library recommendation for mobile application development," *IEEE Access*, vol. 8, pp. 42436–42446, 2020.
[5] S. Zhao, M. Hafeez, and C. M. N. Faisal, "Does ICT diffusion lead to energy efficiency and environmental sustainability in emerging Asian economies?" *Environ. Sci. Pollut. Res.*, vol. 29, no. 8, pp. 12198–12207, Feb. 2022.
[6] M. Michels, W. Fecke, J. Feil, O. Musshoff, F. Lülfs-Baden, and S. Krone, "'Anytime, anyplace, anywhere—A sample selection model of mobile internet adoption in German agriculture," *Agribusiness*, vol. 36, no. 2, pp. 192–207, Feb. 2020.
[7] N. P. Canh, C. Schinckus, S. D. Thanh, and F. C. H. Ling, "Effects of the internet, mobile, and land phones on income inequality and the Kuznets curve: Cross country analysis," *Telecommun. Policy*, vol. 44, no. 10, Nov. 2020, Art. no. 102041.
[8] J. Zhang, "The dynamic linkage between information and communication technology, human development index, and economic growth: Evidence from Asian economies," *Environ. Sci. Pollut. Res.*, vol. 26, no. 26, pp. 26982–26990, Jul. 2019.
[9] Q. Hao, K. Zhu, C. Wang, P. Wang, X. Mo, and Z. Liu, "CFDIL: A context-aware feature deep interaction learning for app recommendation," *Soft Comput.*, vol. 26, no. 10, pp. 4755–4770, May 2022.
[10] J. Schobel, T. Probst, M. Reichert, M. Schickler, and R. Pryss, "Enabling sophisticated lifecycle support for mobile healthcare data collection applications," *IEEE Access*, vol. 7, pp. 61204–61217, 2019.
[11] J. Park, "Evaluating a mobile data-collection system for production information in SMEs," *Comput. Ind.*, vol. 68, pp. 53–64, Apr. 2015.
[12] L. Luo, "Research on the risk and governance of personal information security of mobile internet users in China," *Librarianship Res.*, vol. 13, pp. 37–41, Jul. 2016.
[13] H. Kim, T. Cho, G.-J. Ahn, and J. H. Yi, "Risk assessment of mobile applications based on machine learned malware dataset," *Multimedia Tools Appl.*, vol. 77, no. 4, pp. 5027–5042, Feb. 2018.
[14] F. Ebrahimi, M. Tushev, and A. Mahmoud, "Mobile app privacy in software engineering research: A systematic mapping study," *Inf. Softw. Technol.*, vol. 133, May 2021, Art. no. 106466.
[15] P. Y. He and X. R. Wang, "Research on the privacy and security mechanism of smartphone users: An analysis based on the 'privacy clause' of third-party applications," *Intell. Theory Pract.*, vol. 41, no. 10, pp. 40–46, May 2018.
[16] J. Pan, "Reputation protection mechanism for personal information," *Mod. Jurisprudence*, vol. 43, no. 2, pp. 155–170, Mar. 2021.
[17] T. Sharma, H. A. Dyer, and M. Bashir, "Enabling user-centered privacy controls for mobile applications: COVID-19 perspective," *ACM Trans. Internet Technol.*, vol. 21, no. 1, pp. 1–24, Feb. 2021.
[18] A. Majeed and S. O. Hwang, "A comprehensive analysis of privacy protection techniques developed for COVID-19 pandemic," *IEEE Access*, vol. 9, pp. 164159–164187, 2021.
[19] Y. Zhang, "Criminal law protection of APP personal information: Informed consent as a perspective," *Legal Stud.*, vol. 8, pp. 113–126, Aug. 2020.
[20] Z. B. Hui and Q. L. Qin, "The direction of U.S. Data privacy protection in the post-GDPR era (1970 2019)," China Cyberspace Secur. Develop. Report, Beijing, China, Tech. Rep., 2019, pp. 325–338. [Online]. Available: https://www.pishu.com.cn/skwx_ps/initDatabaseDetail?siteId=14&contentId=11363403&contentType=literature
[21] L. Parker, V. Halter, T. Karliychuk, and Q. Grundy, "How private is your mental health app data? An empirical study of mental health app privacy policies and practices," *Int. J. Law Psychiatry*, vol. 64, pp. 198–204, May 2019.
[22] N. Li and W. D. Li, "Research on personal information security of mobile reading APP users: A survey analysis based on 10 mobile reading APPs," *Librarianship Res.*, vol. 21, no. 11, pp. 48–56, Nov. 2019.
[23] Central People's Government of the People's Republic of China. (2021). *'Fourteenth Five-Year Plan' Information and Communication Industry Development Plan*. SHTML. Accessed: Nov. 1, 2021. [Online]. Available: http://www.gov.cn/zhengce/zhengceku/2021-11/16/content_5651262.htm
[24] X. W. Meng, F. Wang, Y. C. Shi, and Y. J. Zhang, "Mobile user demand acquisition technology and its application," *J. Softw.*, vol. 25, no. 3, pp. 439–456, 2014.
[25] V. M. A. de Lima, A. F. de Araújo, and R. M. Marcacini, "Temporal dynamics of requirements engineering from mobile app reviews," *PeerJ Comput. Sci.*, vol. 8, p. e874, Mar. 2022, doi: 10.7717/peerj-cs.874.
[26] Y. Wang, L. W. Zheng, Y. Y. Zhang, and X. Y. Zhang, "A software requirement mining method for Chinese APP user review data," *Comput. Sci.*, vol. 47, no. 12, pp. 56–64, Dec. 2020.
[27] N. Jha and A. Mahmoud, "Mining non-functional requirements from app store reviews," *Empirical Softw. Eng.*, vol. 24, no. 6, pp. 3659–3695, Jun. 2019.
[28] N. Wang and D. C. Xu, "Investigation and analysis of the current situation of personal information protection in mobile social networks—From the perspective of user behavior," *Intell. Mag.*, vol. 34, no. 1, pp. 185–189, Jan. 2015.
[29] Y. Y. Yang, "Research on the protection of personal credit rights in the context of financial technology," *Southwest Finance*, vol. 1, pp. 3–17, Jan. 2019.
[30] L. Nurgalieva, D. O'Callaghan, and G. Doherty, "Security and privacy of mHealth applications: A scoping review," *IEEE Access*, vol. 8, pp. 104247–104268, 2020.
[31] S. Yoo, H. R. Ryu, H. Yeon, T. Kwon, and Y. Jang, "Visual analytics and visualization for Android security risk," *J. Comput. Lang.*, vol. 53, pp. 9–21, Aug. 2019.
[32] T. A. Coleti, P. L. P. Correa, L. V. L. Filgueiras, and M. Morandini, "TR-model. A metadata profile application for personal data transparency," *IEEE Access*, vol. 8, pp. 75184–75209, 2020.
[33] D. Miorandi, A. Rizzardi, S. Sicari, and A. Coen-Porisini, "Sticky policies: A survey," *IEEE Trans. Knowl. Data Eng.*, vol. 32, no. 12, pp. 2481–2499, Dec. 2020.
[34] X. J. Sun, "Citizens and government in the age of big data," *Leadership Sci.*, vol. 13, p. 21, Jul. 2013.
[35] A. M. Helm and D. Georgatos, "Privacy and mHealth: How mobile health apps fit into a privacy framework not limited to HIPAA," *Syracuse Law Rev.*, vol. 64, no. 1, pp. 131–170, 2014.
[36] K. Huckvale, J. T. Prieto, M. Tilney, P.-J. Benghozi, and J. Car, "Unaddressed privacy risks in accredited health and wellness apps: A cross-sectional systematic assessment," *BMC Med.*, vol. 13, no. 1, pp. 1–13, Sep. 2015.
[37] M. M. H. Onik, C.-S. Kim, N.-Y. Lee, and J. Yang, "Personal information classification on aggregated Android application's permissions," *Appl. Sci.*, vol. 9, no. 19, p. 3997, Sep. 2019.
[38] A. Varanda, L. Santos, R. L. D. C. Costa, A. Oliveira, and C. Rabadão, "Log pseudonymization: Privacy maintenance in practice," *J. Inf. Secur. Appl.*, vol. 63, Dec. 2021, Art. no. 103021.
[39] A. Marwick and E. Hargittai, "Nothing to hide, nothing to lose? Incentives and disincentives to sharing information with institutions online," *Inf., Commun. Soc.*, vol. 22, no. 12, pp. 1697–1713, Oct. 2019.

[40] D. W. Zhang and X. Z. Xie, "The dichotomous interaction of privacy concerns and privacy burnout: An empirical study of digital natives' privacy protection intentions," *Intell. Theory Pract.*, vol. 44, no. 7, pp. 101–110, Mar. 2021.
[41] M. Wang, G. S. Hou, and Z. L. You, "A study on the influencing factors and behavioral choices of internet users' privacy fatigue—Based on S-S-O theory and rooting theory," *Intell. Theory Pract.*, vol. 44, no. 9, pp. 149–154, Apr. 2021.
[42] H. Li, L. Yu, Y. M. Xu, and M. F. Xie, "A study of the social network privacy paradox from the perspective of explanation level theory," *J. Intell.*, vol. 37, no. 1, pp. 1–13, Jan. 2018.
[43] L. H. Peng, H. Li, Y. F. Zhang, and C. Hong, "A study of the factors influencing user privacy and security on mobile social media burnout behavior—A CAC research paradigm based on privacy computing theory," *Intell. Sci.*, vol. 36, no. 9, pp. 96–102, Sep. 2018.
[44] K. O'Loughlin, M. Neary, E. C. Adkins, and S. M. Schueller, "Reviewing the data security and privacy policies of mobile apps for depression," *Internet Intervent.*, vol. 15, pp. 110–115, Mar. 2019.
[45] Y. F. Zhang, Y. X. Wang, and L. H. Peng, "An empirical study on user perception measurement of mobile short video app privacy policy under hard rules," *Intell. Theory Pract.*, vol. 44, no. 7, pp. 94–100, Jul. 2021.
[46] Y. F. Zhang and Y. Qiu, "Research on privacy policy compliance of China's mobile reading app under hard rules," *Mod. Intell.*, vol. 42, no. 1, pp. 167–176, Jan. 2022.
[47] Y. F. Zhang, Y. L. Liu, and L. H. Peng, "An empirical study on the perception measurement of mobile social media users' privacy policy reading under hard rules," *Library Intell. Work*, vol. 65, no. 4, pp. 49–60, Feb. 2021.
[48] J. M. Smith and G. R. Price, "The logic of animal conflict," *Nature*, vol. 246, no. 5427, pp. 15–18, Jan. 1973.
[49] J. M. Smith, "The theory of games and the evolution of animal conflicts," *J. Theor. Biol.*, vol. 47, no. 1, pp. 209–221, Sep. 1974.
[50] P. Kou, Y. Han, and J. G. Shi, "A study of local government environmental control behavior in the context of central environmental protection inspectors," *Oper. Manage.*, vol. 30, no. 10, pp. 127–133, Oct. 2021.
[51] X. Li, R. Huang, J. Dai, J. Li, and Q. Shen, "Research on the evolutionary game of construction and demolition waste (CDW) recycling units' green behavior, considering remanufacturing capability," *Int. J. Environ. Res. Public Health*, vol. 18, no. 17, p. 9268, Sep. 2021.
[52] Z. H. Yan and X. J. Tang, "Humanistic analysis of drug quality and safety regulation based on evolutionary game," *Manage. Comments*, vol. 33, no. 5, pp. 64–75, Jan. 2021.
[53] X. F. Zhu, X. T. Huang, and G. F. Bian, "Research on the quality control of micro-government information disclosure considering reputation," *Library Theory Pract.*, vol. 5, pp. 6–70, May 2019.
[54] Y. Guo, K. Zou, C. Liu, and Y. Sun, "Study on the evolutionary game of information security supervision in smart cities under different reward and punishment mechanisms," *Discrete Dyn. Nature Soc.*, vol. 2022, pp. 1–14, Apr. 2022.
[55] G. Zhu, H. Liu, J. Chen, and X. M. Du, "A study of privacy accountability in the context of mobile health services—An evolutionary game based perspective," *Mod. Intell.*, vol. 38, no. 12, pp. 32–39, Dec. 2018.
[56] M. Zhou and P. Qian, "Evolutionary game study on the protection and use of personal data of over-collected APPs under government regulation," *Intell. Explor.*, no. 11, pp. 8–18, Dec. 2018.
[57] X. C. Qu and G. S. Hou, "Research on information security governance of platform based on three-party evolutionary game," *Mod. Intell.*, vol. 40, no. 7, pp. 114–125, Jul. 2020.
[58] J. J. Cui, "Reflection on the progress of the standardization of personal information security," *Legal Stud.*, vol. 7, pp. 162–174, Jan. 2020.
[59] X. Cao, J. Yu, and L. P. Zhang, "Study on the factors influencing the stability and evolution of industry-academia-research alliances under different alliance sizes," *Manage. Comments*, vol. 28, no. 2, pp. 3–14, Feb. 2016.