Privacy and Information Disclosure: Dynamic Digital Governance in Response to COVID-19

Yinghui Cai, Beijing Institute of Technology, China*
Xiaotao Zhang, Central University of Finance and Economics, China
Huayong Niu, Beijing Foreign Studies University, China
Wei Li, Central University of Finance and Economics, China
Da Huo, Central University of Finance and Economics, China
Jianing He, International Business College, South China Normal University, China
Hong Chen, School of International Trade and Economics, Central University of Finance and Economics, China

ABSTRACT

The information collection in the global governance of the digital economy is important to companies in response to COVID-19. This research studied the initiative of conflicts between privacy and information disclosure based on agency theory, analyzed the resolution of the conflicts based on incentive compatibility, and further discussed the rationale of the balance between private and public interest based on agile governance. This research suggests the necessity of finding the balance between public interest and privacy protection based on the hierarchical division of private and public interest. The dynamic psychological behavior to privacy and information disclosure by uninfected and infected citizens in response to COVID-19 is simulated by Volterra differential equations. The specification of boundaries in data use can be helpful to companies in reconciling the privacy and information disclosure for customer relationship management in digital governance in response to COVID-19.

KEYWORDS
COVID-19, Digital Governance, Information Disclosure, Privacy, Volterra Differential Equations

INTRODUCTION

After the outbreak of COVID-19 in early 2020, the government immediately set up a leading group for COVID-19 prevention and control. Chinese citizens proved very willing to follow public instructions to efficiently suppress potential outbreaks. When epidemics occur, public administration entities, enterprises, social organisations, and individuals hope to quickly obtain accurate information about the pandemic’s nature, scope, cause of infection, transmission range, and rate of death. If a citizen has a transmittable disease that may be publicly harmful, this information is considered one’s personal privacy. If the information is disclosed, patients may encounter specific difficulties in life and work...
(Yang, 2017). When the relevant public departments are required to publish epidemic information in a timely and accurate manner, they will inevitably use their administrative executive power to collect epidemic-related information. It is necessary to manage patients’ private and personal data in this process. Therefore, in the relevant public departments responsible for collecting and disclosing patients’ personal information, there is bound to be a conflict between the power of administrative law enforcement and the protection of citizens’ civil rights.

Customer management for companies in the service sector has been greatly influenced by the digital governance of private information disclosure in response to COVID-19. Yang (2021) pointed out that the agreement of the collection of personal information by customers is essential to companies in digital governance. Several companies have requirements for customers to scan the two-dimensional barcode to report their travelling records before entering their premises. The psychological preference of individuals for privacy and information disclosure can affect customers’ willingness to enter an establishment. Wang (2020) pointed out that the confidentiality of information disclosure can be crucial to the orientation of personal information protection in online services. Customer management requiring personal information disclosure can further impact the frequency, length, involvement, and consumption of customers in service sectors, including restaurant services, aviation services, bank services, shopping services, training services, and sports and entertainment services. Shen et al. (2022) pointed out that the privacy of data used by companies and the preference of customers in information disclosure can be critical to the competitiveness of companies. Basu Sharma noted that the COVID-19 pandemic has affected every aspect of business and society, including foreign direct investment (FDI). According to an UNCTAD estimate, global FDI flows may have fallen by 40% in 2020–21, with the decline being more severe in developing countries. Looming large are fears of disruptions to supply chains, decelerations of international trade, and concerns over likely takeovers by large multinational corporations (MNCs) and state-owned enterprises to take advantage of the weakened economic situation of companies in many countries (Basu Sharma, 2021). Mario Arturo Ruiz Estrada pointed out that the world economy was used to illuminate and illustrate the applicability of the COVIDECONOMICS-19 simulator, from which analyses provide a coherent evaluation of the degree to which post-COVID-19 negative economic effects on world inflation and unemployment. The psychological preferences of individuals regarding privacy and information disclosure are also essential issues in the regulation of data usage in the digital economy and offer support to the digital governance of companies in response to COVID-19.

**Digital Governance in Notification of COVID-19**

News about COVID-19 is shown on the National Health Commission website to inform citizens. The information covers the number of newly confirmed cases, deaths, suspected cases, and cured and discharged patients in each province. Nevertheless, it does not provide any specific personal information. The information in the notification of provincial health committees is similar to the national information. It contains information about the number of newly confirmed cases, deaths, and suspected and reduced chances in all parts of the country. The notification content in some provinces has rarely shown a different pattern.

The excessive disclosure of personal privacy information can affect individuals (Zhou & Zhou, 2019). The exposure of patient information concerns the revelation of confidential information that is essential to individuals.

Since the COVID-19 outbreak in 2020, people have been required to fill out a paper registration form, scan a registration code or provide a health code on a mobile phone to go to public places such as supermarkets, restaurants and stations to prevent and control the epidemic. Such measures have become a part of daily life. The COVID-19 epidemic has accelerated the application of digital technologies, especially big data and cloud computing, which not only helped epidemic prevention but also promoted the wide application and deep integration of digital technologies in social governance scenarios. Yin and Li (2021) pointed out that citizens have an inviolable right to their personal
information, but people also have the right to know some of the patients’ personal information, such as the tracing information. It is a balance between public interests and personal interests.

**Regulation in Data Use for Public and Private Interests**

As far as the power of administration of the law is concerned, the relevant laws and regulations have some norms for collecting and publishing epidemic information. Nevertheless, the rules are too general and the boundaries are unclear, resulting in a wide variety of data released by relevant departments. As far as protecting citizens’ right to privacy is concerned, the lack of specific procedures and mechanisms leads to the lack of operability of legislation and institutional shortcomings in practice (Cao & Wang, 2020). There are preliminary norms for protecting the right to privacy and personal information in the Civil Code. Nevertheless, they do not solve the conflict with the government’s power to execute the law. The specific analysis of this conflict is as follows.

First, the relevant provisions are stipulated in Chapter III of the Law on the Prevention and Control of Infectious Diseases, “Epidemic Reporting, Notification, and Announcement.” This chapter only provides the explicit obligation of the relevant public agencies to report the epidemic and requires institutions to disclose epidemic information, as stated in Article 38. According to the existing regulations, the law does not provide detailed rules for how relevant public departments collect information concerning epidemics. Neither does it establish exact procedures for releasing epidemic information at the municipal, county, or township levels. For the release of epidemic information on infectious diseases, the general legal provision is that “it shall be released timely and accurate,” without mentioning any other specific requirements.

Second, the relevant provisions of the Regulations on the Disclosure of Public Information. Article 20, Item 12 of the Regulations stipulates that the public shall take the initiative to disclose the information concerning emergency plans, early warning, and response to in cases of public emergencies. Article 15 stipulates that the administrative organ shall not disclose public information involving trade secrets and personal privacy that may harm the legitimate rights and interests of a third party. However, the administrative organ shall disclose public information if the third party agrees. If the administrative organ considers declaring the news, it will significantly impact the public interest. The Regulations on The Disclosure of Public Information does not define whether epidemic information should be disclosed voluntarily to the public, nor does it stipulate under what circumstances information involving personal information and privacy in epidemic information should be disclosed.

Third, there is a certain ambiguity in the relevant provisions of Chapter VI of the Civil Code on Personal Rights. The Civil Code has relatively comprehensive requirements for protecting privacy and personal information, which forbid organisations and individuals from violating privacy rights and forbid illegal collection and processing of personal data. Therefore, it is clear that state organs and their employees shall keep private and personal information confidential. However, there is no clear mandate for the state administration to collect citizens’ private and personal data.

Fourth, Article 13 of the Personal Information Protection Law states that the relevant public departments may make reasonable use of personal information if it is necessary to respond to public health emergencies or protect the life, health, and property safety of citizens in emergencies. Articles 34 and 35 stipulate the general processing of personal information by state organs. However, there is still room for improvement in future laws on how to design operational regulations reasonably so that the protection of personal information is guaranteed without affecting the collection, processing, and disclosure of epidemic-related information by administrative organs according to the law.

Therefore, through legislative norms, it has become an important issue to be solved in the PRC’s legislation, namely, to resolve the conflict and to determine the boundaries between the administrative right to execute the law (or the public’s right to know) and the protection of personal information and privacy rights in cases of public emergencies. Therefore, according to the relevant provisions of the current law and the empirical investigation of the disclosure of epidemic information, this article provides a detailed account of the following issues.
First, in the information society, what methods and procedures can relevant public departments use to collect, for instance, information concerning epidemics? Second, what legal guidelines and principles should the public follow when using these methods? Third, how should relevant public departments protect personal privacy and information if publishing epidemic information is required?

Second, how do we define the public’s right to obtain relevant and accurate information about the epidemic? What principles should relevant public departments follow when disclosing epidemic information to ensure that the public receives sufficient information and, at the same time, to guarantee the security of personal and private information?

Third, how can the relevant provisions of the law on the Prevention and Control of Infectious Diseases and the Regulations on the Disclosure of Public Information, which involve the protection of personal privacy, be improved? In the same vein, how can the law’s relevant provisions on the protection of personal information that concerns public events and other exceptional cases that may involve personal information be reasonably designed?

INFORMATION DISCLOSURE IN RESPONSE TO COVID-19

Having analysed other countries’ legislation, such as that of the European Union, the United States, and other countries and regions with relatively developed data protection and utilisation rules that have established regulations for personal processing information in public events in legislation or jurisprudence, we found that they mainly include the following criteria and regulations.

Partial Disclosure of Private Information to the Public

The theoretical foundation of respecting the subject’s consent lies in the dignity of the human person, which reflects the right of citizens to control and dispose of personal information freely (Xu, 2019). Based on this, the General Data Protection Regulation of the European Union establishes the principle of informed consent of data subjects under general circumstances. It provides six types of reasons for processing personal information without the consent of data subjects. In the U.S., the Health Insurance Carrying and Liability Act (HIPAA) provides the disclosure and use of health information without personal consent in 12 categories involving national interests, including public health events, health regulatory activities, health or safety risk reduction, and essential public work. HIPPA-regulated identifiable personal health information covers individual and aggregate information, including past, present, and future physical and mental health information, relevant payment information, and demographic statistics.

Data Security by Third Party Authorities

“Third-party guidelines” apply to third-party institutions (hospitals, telecommunication carriers, insurance companies, etc.) that provide personal information in their possession at the request of public departments, which are not subject to the Fourth Amendment to the U.S. Constitution (exempting citizens from unreasonable searches and seizures). This principle is applied by U.S. courts in data assistance obligations, and it also applies to activities such as mandatory reporting of health data. The data collector can change the user’s purpose when collecting without the user’s consent and disclose the data to public departments at one time or regularly.

With the rise of digital platforms to handle massive amounts of user data, there will be an increased number of scenarios in which data are used for public welfare purposes. Take influenza prevention and treatment as an example. Many user-based platforms in the United States are actively using poverty, unemployment, low education, housing instability, and food insecurity as criteria for high-risk group identification. These data can help the medical industry predict influenza incidents and admission rates more accurately, promote medical care and promote the effective distribution of medical resources. Third-party guidelines should be considered, as they provide a framework for using massive data for law enforcement and public welfare purposes.
Fine Balance Between Privacy and Necessary Information Disclosure

Both the public interest and “third-party guidelines” serve as legal principles that aim to balance the use and protection of information and diminish conflicts of interest. Nevertheless, they fail to solve the problem of how to demarcate specific boundaries in reality. Instead, they highlight the potential conflict between two values: an individual’s right to privacy and the public interest in disclosing public information (Zhang, 2008). How to balance these two in different scenarios will largely depend on proportionality; that is, a reasonable compromise between public needs and public interests should be found, considering the extent to which personal information may be released.

In the context of the epidemic, information openness and transparency play an important role in the prevention and control of the epidemic. However, in the process of epidemic prevention and control, the protection of citizens’ personal information privacy also needs to be given important consideration. In the context of epidemic prevention and control, the principle of information subject to consent can no longer be used as a legitimate reason for violating citizens’ personal information, and the public interest is an alternative option (Jiang, 2020).

Considerable data utilisation is a typical example of a conflict of interest, which has received more attention in recent years. Judge Rubenstein of the U.S. Federal Court pointed out that ample data use has brought challenges to privacy protection laws. On the one hand, it blurs the boundaries of personal and nonpersonal information, and, on the other hand, it impacts the principles of information minimisation and informed consent. Health or big medical data is such an example. Big Data concerning health is generally regarded as the most personal and confidential information. Nevertheless, it is also valuable information that can be used for suspect identification, epidemic research, public policy formulation, and biomedical and behavioural research. In the future, more diversified data applications are bound to be generated in the field of big health data, and the delineation of personal information utilisation and protection will face more challenges.

REGULATION OF BIG DATA USE IN RESPONSE TO COVID-19

The Legitimacy of the Use of Big Data Technology

From the perspective of the prevention and control of public health emergencies, the effectiveness of epidemic prevention and control needs to rely heavily on monitoring, collecting, reporting, interpreting, and releasing mechanisms of epidemic information. Only based on timely, accurate, and complete information access and processing mechanisms can scientific, practical, and urgent decision-making be supported and implemented in various specific measures. While collecting personal information, the public often uses modern technical means such as big data to obtain mobile communication data, such as mobile roaming information and internet data. Regarding the practice of being reported by others and relevant departments and institutions taking the initiative to conduct investigations, the “infectious disease prevention act” and the Regulations on The Emergency Response to Public Health Emergencies both stipulate that any unit, community, or individual “has the right to report hidden dangers of emergencies to the public and relevant departments.” Furthermore, “when infected patients or those who are suspected of having the infectious disease are discovered, they should be reported to a nearby disease control and prevention agency or medical institution immediately.” There are no clear regulations on collecting big data from devices such as mobile phones or mobile internet and traffic data, which is also the most likely situation of excessive collection of personal information. More target-oriented policies and rules are urgently needed.

To prevent and control the epidemic, on the one hand, it is necessary to monitor and manage people’s movements across the country and in critical areas with the help of large-scale extensive data analysis and conduct situation research with subsequent investigation, prediction, and early warning when needed. It is also necessary to improve the refinement and accuracy in the policy implementation process. On the other hand, measures should be provided according to the story
within the classification for people who are proven to have different levels of substantial risks. According to the National Public Health Emergency Plan issued in 2006, “Prevention work is taken for the travellers, control measures are implemented, on-site isolation, on-site observation, and on-site treatment measures are taken for patients, and those who are suspected of being infected with transmittable diseases, and centralised or home medical observation is taken for those who had close contacts with them according to the situation.”

From the statements of the government and enterprises, the information of the first group mentioned above will be processed, and the anonymity of this personal information is emphasised and guaranteed. The information is only used to analyse the situation. The use of the personal information of the second group involves the processes of storage, tracking, and analysis based on risk evaluation. In addition, corresponding measures based on the study of the information, need to be taken against individuals. These measures will restrict individual freedom of conduct. Coercive measures can also be taken if individuals refuse to cooperate, and in severe cases, criminal sanctions may be applied.

Modern technical means to collect epidemic information and promote epidemic governance can improve governance with the help of the technical advantages of big data in local fields. Nevertheless, these technical means now penetrate everyone’s daily life as never before. Therefore, if there is no moderation, especially if respect for privacy and personal information is not maintained, it may result in insecurity and resistance to being “under constant supervision.”

**Governance in the Regulation of Big Data Use**

When collecting and processing citizens’ personal information, the public should follow the principle of due process, that is, strictly follow legal procedures (Liu, 2018). Especially in collecting, reporting, transmitting, and personal feedback information without individual consent, standardised mechanisms and means need to be established.

First, although any unit/community or individual has the right or even the obligation to “report,” the receiving reports should be as centralised and standardised as possible so that timely announcements can be made to society. In cases in which personal information collection is concerned, it should be stored appropriately and kept confidential. Basic training should be provided for relevant staff to avoid the unrestricted mass distribution of personal information on the internet. When personal information is disclosed, the responsible relevant staff should be punished. Nevertheless, a penalty in a broader standardised mechanism, such as operating specific processes and disciplinary frameworks, needs to be urgently implemented.

Second, for assessing specific groups of people with risks, after determining that corresponding measures have been taken, the principle of minimising their personal information should also be used according to the situation, such as limiting the range of people who have access to their mobile phone numbers, specific addresses, and identity information as much as possible to avoid excessive interference with relevant groups of risk. When it is necessary to publish information on a broader scale for early warning, it should also be anonymised. Only the place, time, and related precautions required for early warning should be targeted or disclosed to a certain extent, without the need to include information that can identify individuals. After processing, personally sensitive information has unrecognised characteristics to avoid the trouble caused by private information leakage (Kong, 2020).

**Principles of Information Disclosure to the Public**

According to Article 33 of the infectious disease prevention act, disease prevention and control institutions shall take the initiative to collect, analyse, investigate and verify epidemic information and report it to the health administration department. Although individual rights and freedom of movement are appropriately made secondary to the public interest, which is not only a situation stipulated by laws and regulations but also a policy that is readily accepted by the public intuitively and intellectually, in such a case, the “information” attributing personal information is also essential. As the fundamental supporting element of epidemic prevention and control, epidemic information
inevitably includes collecting, processing, and transmitting massive amounts of personal details because people are the basic units and carriers of epidemic transmission.

In personal information protection, the much-debated relationship between “public security” and “personal interests” is intensely scrutinised, as if under a magnifying glass during this particular period. As part of the epidemic information and prevention and control mechanism, it is inevitable for individuals to give up their rights and interests, including personal information, to control and secure overall risks.

Article 1035 of the Civil Code stipulates that the processing of personal information shall follow the principles of legality, legitimacy, and necessity and shall not be excessively processed. Unless the contrary is prescribed by law or administrative law, the consent of a citizen or his guardian shall be obtained. Article 1027 stipulates that citizens may consult or copy their personal information from the information processor by law. If they find that the data are wrong, they have the right to object and request timely correction or other necessary actions. If the information processors violate laws and administrative regulations or the agreement between the two parties to process their personal information, they have the right to request the information processor to delete it in a timely manner. The Civil Code stipulates that the subjects of civil law have the right to informed consent, access, reproduction (acquisition of copies), correction, and deletion. These provisions have covered the privileges enjoyed by the subjects of civil law throughout the life cycle of personal information and established the control of civil law issues over the use and circulation of their data, rather than just leaving this right at the declaration level.

The fundamental law in civil and commercial affairs stipulates that there are only eight specific provisions for privacy rights and personal information protection in the Civil Code that establish basic rules, providing the foundation for other legislation and leaving room for future development, making it relatively flexible. However, the law must finally be applied in practice. Therefore, the provisions on privacy and personal information protection of the Civil Code need to be implemented in judicial training and need to be further refined in subsequent relevant legislation:

1. **Clarify Liability for Necessary Information Disclosure:** In judicial practice, there is a particular liability for personal information infringement. For example, when personal information is illegally disclosed, the victim cannot prove the leaker’s identity. Referring to the specific personality right and general tort liability often makes it difficult for the subjects of civil law to protect their interests. At present, only Article 55 of the Consumer Protection Act stipulates that if a business operator infringes on the human dignity of consumers, infringes on the personal freedom of consumers, or infringes on the right of consumers’ personal information, which is protected according to law, they shall stop the infringement, restore reputation, eliminate the impact, apologise, and compensate for losses and eliminate future dangerous liability. As a new type of tort, the Civil Code does not stipulate the attribution principle, constituent elements, or how to bear tort liability for infringement of personal information, which should be further improved in subsequent supporting legislation acts.

2. **Identify Reasonable Operation of Personal Information:** Article 1036 of the Civil Code stipulates that the balance between the protection of personal information and the fair use and free flow of personal data should be considered when dealing with situations in which personal data can be exempted from liability. How is “reasonable” judged? What is not “excessive”? For example, information such as gender, age, surname, whereabouts, and the specific nature of activities of COVID-19 patients will be released to the public, including personal home address, ticket, and flight information. Is this behaviour reasonable or excessive? In general, “reasonable” is equivalent to the principle of purpose limitation. The operation beyond the original purpose of personal processing information is unreasonable and is no longer exempt from liability. However, it is not explicitly stipulated in the Civil Code and leaves it for further improvement in practice.
3. **Understand the Processor of Personal Information:** The Civil Code stipulates that the compulsory subject responsible for protecting personal information is the “information processor, not any organisation or individual.” It also further specifies that the processing of personal information includes the whole lifecycle process of collection, storage, use, processing, transmission, provision, disclosure, etc. Is any action involving the collection of personal information? For example, is installing cameras in the outpatient hall of the hospital where patients enter, which permits naturally obtaining information about an individual’s appearance, part of the handling behaviour stipulated in the Civil Code? If you enter a park gate, the door of a hotel, or a convenience store, the doorman requires you to provide your personal information. Is the doorman an information processor? Is requiring children and family members to fill in the health information form in kindergartens and primary schools part of the information processing stipulated in the Civil Code? Parents collect their children’s personal information and report it to the school. Are parents’ information processors? National legislation, such as the E.U. General Data Protection Regulations (GDPR), stipulates that information processors not include ordinary natural persons. The processing of personal information in individual or family activities is not within the legal scope; however, the Civil Code does not stipulate it and when the Civil Code applies needs to be further clarified.

To ensure the legitimacy of the behaviour used to collect personal information in special periods such as an epidemic, it is suggested that the following basic principles be applied. First, the collection of personal information must directly point to the purpose of infectious disease prevention and control, such as account passwords, property information, credit information, transaction information, secret finger models, and other information unrelated to this purpose, which are not included in the collection. Second, the collected data must be reasonable, and the sense of the prevention and control of infectious diseases, such as managing the whereabouts of patients, suspected patients, pathogen carriers and close contacts during the incubation period of the virus, and the whereabouts beyond the average incubation period recognised by medical recognition should not fall within the scope of collectability. Third, there must be no other way to collect personal information. To achieve the stated purpose of prevention and control, it is hoped that the public authorities will collect personal information as the last option to perform a specific goal. Fourth, when collecting personal information, the information subject must be informed of the purpose and scope of the collection, which guarantees the subject’s right to know and limits information collection and use of the subject’s self-discipline to prevent random collection and usage.

**RESOLUTION OF THE CONFLICT BETWEEN PRIVACY AND INFORMATION DISCLOSURE**

Citizens’ right to complete information includes not only the individual’s right to obtain public information from the public, it also includes the right to know and the right of citizens to independently decide the extent to which to disclose the facts of their personal lives to the public (Zhao, 2017). The right to privacy in modern society refers to subjects’ right to control the flow of their personal information. The scope of personal privacy includes personal information and personal space and activities (Yang, 2017). The right to know is a prerequisite for freedom of information. Any citizen is entitled to know all information held by the public related to exercising his power (Wang, 2014). Everyone not only hopes that their personal information will not be leaked but also, as a member of society, hopes to know more information to meet their own needs.

The resolution of the conflict of privacy and information disclosure in customer services for companies is vital to managing customer relationships in the global market. Cavusgil et al. (2005) pointed out that the relationship management of companies is a critical research stream in an ontological study in the international marketing area. Liu and Gao (2016) pointed out that the privacy
protection of companies can offer support to customer relationship management based on enhanced brand equity and trust relationships by customers in online services. Park et al. (2012) concluded that reward-seeking psychological behaviour is an essential motivation for individuals to reconcile the conflict of privacy and information disclosure in customer relationship management of online services. Li et al. (2016) found that reasonable use of private information to improve customer services and enhance the quality experience is compatible with individual interests and understandable to customers in relationship management of online services.

During the pandemic, the conflict between the right to privacy and the right to information has become significant. Balancing the rights related to information disclosure reflects the difficulties faced by the government in managing this tension.

**Conflict of Information Disclosure Based on Agency Theory**

The conflict between the right to privacy of personal information and the right to information of public interests can be regarded as an agency problem in public health emergencies. The conflict between the two rights is more apparent based on agency theory.

First, the conflict between the two is mainly reflected in the conflicts of interest between the public and individuals. In the case of public emergencies, the collection and analysis of relevant information is an essential strategic information resource to accurately study and judge the current situation and formulate appropriate coping strategies. In the view of the public, only when sufficient information is obtained can the public and other relevant institutions effectively deal with emergencies. They can also make the best choice to reduce the risk accordingly. Therefore, the public has a strong demand to publish and disseminate relevant information through a wide range of media channels. However, this kind of information resource is also related to personal privacy to a great extent. At the same time, with the rapid development of social media, the channels and accuracy of information dissemination are not entirely controllable, which will cause serious trouble for individuals and even cause them to suffer illegal violations. Therefore, individuals have a strong sense of unease about the multichannel and high-speed dissemination of relevant information. Based on the above analysis, the protection of the public’s right to know directly depends on disclosing personally relevant information. Therefore, the protection of personal privacy will infringe upon the public's right to know. Thus, the interests of the public and individuals are not consistent or even conflict with each other. In the case of conflicts of interest and under the pressure of emergencies, it is easy for information holders to infringe upon personal privacy to meet the excessive needs of the public’s right to know, which may lead to agency problems.

Second, the conflict is based on the information asymmetry between the two sides. To deal with emergencies, individuals provide privacy and other relevant information to the government or other information demanders to seek help. If the information holder cannot accurately grasp the yardstick of information disclosure or excessive disclosure of information to appease the public or if excessive acquisition and dissemination of personal information by the public to meet their interests infringe upon individual privacy, the agency problem arises (Liu & Jiang, 2006).

During the epidemic, the public inevitably panics, so disclosing relevant information about epidemic-related personnel enhances public understanding of the spread of the epidemic and prevention and control measures and is an important channel to maintain social order and stability. Second, citizens can make correct decisions according to relevant information as rational individuals. The disclosure of information is also an effective measure to improve epidemic prevention awareness and control the development of the epidemic from the perspective of the masses (Yang & Guan, 2021).

Therefore, disclosing relevant information about the people involved in the epidemic is conducive to stabilising the epidemic and maintaining social order, and the public’s right to know takes precedence. However, to meet the needs of epidemic prevention and control, public administrative entities and other relevant departments use personal information, such as names, identity card numbers, medical records, and work units, and this information is closely related to personal property
safety and even personal safety, especially today when big data are developing rapidly. If random announcements are made, epidemic-related personnel will face many unknown risks and be under heavy psychological pressure. Therefore, people involved in the epidemic have an equally strong desire to protect their private information.

The publication of relevant information about the people involved in the epidemic has become a point of contention between the interests of individuals and the public. In real life, COVID-19’s long incubation period and strong infectivity make people very sensitive to the relevant information of patients to meet the need for self-protection, resulting in excessive demands for the right to know. When confirmed cases are verified, the public’s demand for relevant information is beyond the scope established by the government and other institutions. It is excavated and disseminated through various media to disclose unnecessary information for epidemic prevention and control. Even rumours appear, which pose a significant challenge to individuals’ right to privacy. At the same time, highly developed social media, the pursuit of excessive details in media reports, and the high degree of panic or curiosity of the public all aggravate the possibility of illegal acquisition and dissemination of private information; thus, during the epidemic, the conflict between personal privacy and the public’s right to know is particularly acute.

Resolution to Balance Conflict Based on Incentive Compatibility

The contradiction between individual privacy and the public’s right to know is also a conflict and contradiction between personal interests and collective interests, and incentive compatibility is a common way to solve such inconsistencies. That is, it establishes a mechanism that maximises individual interests and allows organisations to achieve the goal of value maximisation (Zhou, 2018). The conflict between personal privacy and the public’s right to know is not irreconcilable. According to the principle of incentive compatibility, the rational publication of personal information is an effective mechanism to maximise the value of both sides. On the one hand, as long as the information disclosure system is reasonable enough, the individual’s right to privacy can be effectively protected to avoid the possible negative impact of unreasonable dissemination of information. Personal resistance to information disclosure will be greatly weakened. On the other hand, if the vital information related to the public interest is reasonably disclosed, it will not hinder the realisation of the public interest goal. As a result, a mechanism that considers personal privacy and the general right to know has been established.

Information Disclosure to the Public Based on Agile Governance

The concept of agile governance was raised at the World Economic Forum in 2018. (Peng, 2022) In the era of the Fourth Industrial Revolution, the shortcomings mentioned above of top-down governance mechanisms can be overcome through the development of flexible, evolving, and adaptive alternatives in collaboration with the implementing actors. We need new decision-making processes that are more flexible, more inclusive and sustainable. The term “agile governance” itself sets the expectation that this model needs and should keep pace with the rapid changes in society.

With the arrival of the big data era, agile governance has been given new connotations and meaning. In dealing with public emergencies, agile government refers to the process in which government entities and other relevant institutions break through the tradition, make use of the sufficient data resources of the big data era, and actively increase the participation of diversified subjects in the process of dealing with risks in an uncertain environment. The whole process is characterised by multiple issues, a wide range of governance, firm dynamics, and rich data (Xue & Zhao, 2019).

According to the principle of agile governance, the role of data has been greatly improved, which further illustrates the importance of information disclosure in dealing with public emergencies. At the same time, the protection of the public’s right to information is also a pivotal point to further enhance the participation of diversified subjects and form a key point of mass prevention and governance. In
the atmosphere of diversified public involvement, the disclosure of personal information has become a common need for individuals and the public to achieve their goals. Agile governance focuses on the role of data resources and data technology. To solve many problems, such as epidemic reporting and correction, routine surveillance and early warning of emergencies, automatic early warning and forecasting of surveillance results, spatial distribution of monitoring and analysis data, and epidemic report management of the floating population. (Yan & Tang, 2021. Agile governance prioritises the promotion of social welfare and value proposition to guide a resilient balance between innovation and regulation in cutting-edge technologies. In terms of the public interest, it considers how the government can react and intervene more quickly to minimise the risk of the virus spreading (Shams, R., Vrontis, D., Belyaeva, Z., Ferraris, A., & Czinkota, M. R., 2020).

Rational Boundary of Information Disclosure for COVID-19

During the epidemic, the relationship between individuals and the public has become closer. Individuals cooperating with the national epidemic prevention and control measures by reporting their relevant information according to the regulations can speed up medical treatment, which contributes to protecting their own lives and health but is also a basic obligation as a citizen. At the same time, after the information reporting mechanism is established, it will also promote the construction of the “fence” of epidemic prevention and control in the whole country, and the continuous improvement of the degree of epidemic prevention and control can also provide more long-term protection for individuals’ right to life and health.

For the public, information resources about the epidemic are essential for understanding the current situation of the epidemic, resolving anxiety, and stabilising social order. It is also an effective tool for improving the speed of the investigation and preventing the spread of the virus. Based on the overlap of interests between individuals and the public, it is indispensable to establish an information disclosure system to address the epidemic. This information disclosure system must follow the principle of “broad entry and strict exit.” Based on the effective collection of information, we should strengthen the management of data, strictly control the public channels and methods of communication, and protect patient information with a high degree of protection (Tang, 2020).

In this way, it can provide sufficient information support for epidemic prevention and protect the individual’s right to privacy. In addition, the traditional top-down management method cannot cope with the complexity and urgency of epidemic transmission under epidemic conditions. Therefore, a new agile governance mechanism is necessary (Yan, etc., 2021). On the one hand, to form a governance method of mass prevention and control, we cannot rely solely on public agencies. On the other hand, in mass participation in epidemic prevention and control, the recognition of information disclosure has been dramatically improved, and the supporting role of data has been affirmed. Individuals are both beneficiaries of and participants in epidemic prevention and control. Personal and public interests are closely related, and the interest gap between information disclosure can be bridged. Therefore, individuals and the public can accept the rational disclosure of information.

Article 15 of the Regulations on the Disclosure of Public Information states that administrative organs shall not disclose public information involving trade secrets, personal privacy, and other disclosures that will cause damage to the legitimate rights and interests of third parties. However, suppose a third party agrees to disclose it or the administrative organ believes that nondisclosure will significantly impact the public interest. In that case, it shall make it public. This article establishes an exception system to disclose personal information, balancing the public’s right to know and personal privacy. A further boundary can be identified between the public interest as a purpose and the disclosure of personal privacy as a means. The proper disclosure of private information in response to COVID-19 is vital to the public.

1. **Hierarchical Division of Privacy and Public Interest:** From the perspective of current legal technology, when there is a conflict between the right to privacy of personal information and
the right to know of the public interest, a balance between protecting individual rights and safeguarding the public interest is generally sought by the principle of proportionality.

Personal information is a collection of various information pointing to a specific subject. The relevance and directionality of this information to a particular person are called identification. The greater the risk of identification, the more serious the impact of identification consequences for individuals, and the higher the protection level of the privacy information should be. The protection of personal privacy information can be divided into three groups. The first level involves highly private information of individuals, such as fingerprints and other biometric information, personal medical records, bank account passwords, and personal tracking data. Such information involves personal safety and personal property security and should be protected at the highest level. The second level identifies specific people, such as gender, height, marital status, criminal record, social relations, academic qualifications, and work experience. Such information should be protected at the middle level. The third level is the information used to contact individuals, such as telephone numbers, mailboxes, and social accounts. This kind of information has social characteristics. The subject of rights will generally take the initiative to disclose it to specific people to be protected at a lower level.

Articles 20 and 21 of the Regulations on the Disclosure of Public Information state that the public’s information may be divided into the following three types. First, it involves the income and expenditure management of public financial funds. The second type consists of the operation of administrative power and the allocation of public resources, and the third type of information is related to public safety and public health. Among the above general information, the public interest that can be reflected is first manifested in public health, public safety, and environmental protection. These are the most basic rights related to human beings’ right to life and health, classified as vital public interests. Second, the public interest involving social and economic development and the construction of public infrastructure is significant public interest. Finally, it is a general public interest involving citizens’ supervision of public functions, the allocation of public resources, and participation in the management of social life.

Through the above division of personal privacy information and the public interest at different levels, it is operable for us to delimit the right to know in public law and interfere with the right to privacy in private law. The higher the level of protection of personal privacy information, the greater the public interest as the subject matter of disclosure of the data. For first-level information involving personal property security, personal security, and private security (such as personal biometric information, medical records, account passwords, property status, and whereabouts), due to the highest intensity of protection, only vital public interests involving public health, public safety, and environmental protection are considered. Only in this way can it be the exception to the nondisclosure of this information. Second-level information (gender, height, marital status, criminal record, social relationship, education background, and work experience) related to the identification of specific individuals with moderate protection intensity can be exempted from disclosure by vital public interests related to social and economic development and operation and public infrastructure construction. Its protection intensity is weak for third-level information used to contact individuals (telephone, email, and social accounts). The general public interest can become an exception to the nondisclosure of this information.

2. The Boundary of Information Disclosure in COVID-19: With the approval of the State Council, the National Health Commission decided to include pneumonia caused by the novel coronavirus in the statutory B-type infectious disease and take preventive and control measures for Class A contagious diseases. Because the virus transmitted by the epidemic is a new virus, at the time of the outbreak of the epidemic, the source of transmission, transmission route, transmission intensity, whether it mutates, etc., of the virus had not been known by the health department. Therefore, to prevent the spread of the epidemic, the government has made public
the relevant personal information of confirmed infected patients, which is conducive to their knowing. Whether there is a risk of infection, taking effective self-protection measures promptly will safeguard the public interest in terms of the lives, health, and safety of the population. It is also the public’s responsibility to perform social management.

The government may need to authorise the disclosure of necessary personal information to protect vital public interests such as public health and safety. At the same time, Articles 12 and 68 of the Infectious Disease Prevention Act also clearly stipulate that relevant information involving personal privacy shall not be disclosed. This brings about how to master the scope of public personal data without revealing personal information. The author believes that since the law stipulates that the public interest is an exception to the nondisclosure of personal information, the limited space for personal privacy has been gradually reduced. To prevent excessive infringement of the disclosure of public information on personal privacy, and according to the principle of proportionality, two elements should also be considered when disclosing personal data: first, personal privacy letters and whether the disclosure of interest is necessarily related to the public interest; and second, whether the means of revealing personal information are reasonable.

3. Identify the Scope of Public Interest: Focusing on the purpose of ensuring public health and safety, combined with the above two elements, the following analysis is made on how to grasp the scope of public personal information during the epidemic.

Concerning the scope of public subjects, the official statistics include four types of cases in this epidemic: confirmed, suspected, cured, and dead. Disclosure of personal information on confirmed cases is conducive to the public knowing whether they have ever been in contact with patients and are at risk of infection to take self-protection measures. Therefore, it is necessary to disclose the personal information of such patients for disclosure. However, should the personal information of suspected patients also be disclosed? Even if patient information is declared based on public interest considerations, the scope and manner of disclosure should be determined according to the degree of exposure (Yang, 2017). The author believes that because this category of patients discloses their personal information before diagnosis, they will be alienated and rejected by the public, facing the risk of social discrimination. If the patient is not diagnosed in the future, the cost of integration into everyday living will increase due to the disclosure of personal information.

Moreover, with technological progress, the waiting time for diagnosis has been reduced to one day. Therefore, it is not too late to disclose the personal information of such patients after they are diagnosed. Thus, revealing the personal information of suspected patients is not a necessity for disclosure purposes. Therefore, such patients’ personal information should not fall within the scope of the disclosure.

Concerning the scope of public information, even the first-level personal information with the highest protection intensity does not need to be disclosed if it is not necessary to achieve the purpose of the disclosure. Therefore, the personal data required for disclosure are the patient’s permanent residence and the patient’s trajectory. It is necessary to ensure that relevant public departments collect targeted information on people in contact to prevent the spread of the epidemic. At the same time, through the above information, the public can know whether they have been in contact with patients. If so, they can take corresponding measures as soon as possible or judge whether they should see a doctor at a time when symptoms appear. Therefore, the disclosure of this information is conducive to maximising the public interest in public health. Although names are the most identifying personal information, they are not required to be disclosed because the public is only concerned with their own risk and does not need to know the name of a particular person. It does not meet the criteria of the most extenuating measures.
In the face of the sudden epidemic, while we are vigilant against the carrier of the virus, we are unwilling to see a large number of patients’ personal information leaked, which puts lawyers in a dilemma between the right to privacy and the right to know. Disclosure of the public’s information without considering the willingness of individuals to keep their information confidential will reduce citizens’ willingness to cooperate with the public (Wang, 2014). The author believes that as personal information in private law, it should not be disclosed in principle. However, as is the case with the right to know in public law, interference with private rights must have clear boundaries. The clearer the scope of publicly available personal information and the clearer the judgement criteria for the public interest are, the more appropriate it is to weigh the two to better grasp the scope and boundaries of information disclosure and to better obtain the scope and limitations of information disclosure.

In summary, because of the conflict between personal privacy and the public’s right to information, it can be analysed and studied according to the following logic and proposed corresponding solutions in Figure 1.

**PSYCHOLOGICAL SHIFTS IN COVID-19 BASED ON VOLTERRA EQUATIONS**

The dynamic shifts in psychological preferences between privacy and information disclosure can be further studied following Volterra differential equations. Lan et al. (2012) argued that firm operations could be developed in the dynamic context of the environment, organisation, and humans based on context theory. The dynamic attitudes of citizens to privacy and information disclosure during COVID-19 are further revealed by switching preferences between private and public interests for infected citizens and uninfected citizens in different contexts by simulation based on Volterra differential equations. Adner and Kapoor (2010) considered that the ecosystem of companies is essential in the value creation of corporate innovation. Yin et al. (2020) studied the industrial competition of firms in innovation based on a simulation of a dynamic ecosystem. Volterra differential equations have been applied to analyse the context of corporate behaviour in the vibrant ecosystem of

*Figure 1. Framework for Resolution to Conflict of Privacy and Information Disclosure in Response to COVID-19*
the digital economy. Man et al. (2011) studied the context of mobile commerce alliances in a dynamic ecosystem based on Volterra differential equations. The Volterra differential equations are as follows.

$Q_{\text{uninfect}}$ represents the number of uninfect citizens who prefer information disclosure in response to COVID-19, and $Q_{\text{infect}}$ represents the number of infect citizens who adversely prioritise individuals’ privacy in COVID-19. The attitudes of infect and uninfect citizens towards privacy and information disclosure can shift due to the environment of residential communities.

For a psychological response of uninfect citizens, the number of uninfect citizens who prefer information disclosure during COVID-19 is increased as the epidemic expands, and the parameter in the growth of uninfect citizens supporting information disclosure is represented by $\alpha$. However, if COVID-19 infects a family member of an uninfect citizen, the attitude of the uninfect citizen will change. As a result, the uninfect citizen shows a higher level of understanding of the right to privacy, and the number of uninfect citizens who support information disclosure will decrease by parameter $\delta$.

For a psychological response of infect citizens, the number of infect citizens who prefer privacy in COVID-19 shows a gradual understanding of the necessity of information disclosure for the public interest, and the number of infect citizens who oppose information disclosure decreases by parameter $\beta$. However, if the infect citizen has a family member who is an uninfect citizen, the attitude of the infect citizen will change. The infect citizen will be more deeply concerned about the family’s privacy, and the number of infect citizens who prefer privacy will increase by parameter $\epsilon$.

The simulation of the psychological behaviour related to privacy and information disclosure in response to COVID-19 by infect and uninfect citizens is summarised in the following cases in Table 1. Table 1 shows the conditions in a case study of the dynamic psychological preferences for privacy and information disclosure by uninfect citizens and infect citizens in response to COVID-19.

In Case 1 there are 2,000 uninfect citizens and 200 infect citizens in a residential community, with a 10:1 ratio of uninfect citizens to infect citizens. Uninfect citizens prefer information disclosure, while infect citizens prefer privacy. The growth rate of uninfect citizens supporting information disclosure is $\alpha$. The decreasing rate of uninfect citizens supporting information disclosure due to a psychological shift to preferring privacy with family members infected is a parameter $\delta$ at 0.02.

Conversely, the decreasing rate of infect citizens who prefer privacy is $\beta$. The growth rate of infect citizens opposing information disclosure due to a psychological shift to choosing privacy with uninfect family members is $\epsilon$. The simulation of the psychological shift to privacy and information disclosure by uninfect citizens and infect citizens is shown in Figure 2.

Case 2 further sets the growth rate of infect citizens who prefer privacy $\epsilon$ from 0.008 to 0.03 due to a more serious concern for the privacy of uninfect family members. The simulation of Case 2 is shown in Figure 3. It is found that the cyclical shifts in psychological behaviour related

<table>
<thead>
<tr>
<th>Case</th>
<th>$Q_{\text{uninfect}}$</th>
<th>$Q_{\text{infect}}$</th>
<th>$\alpha$</th>
<th>$\delta$</th>
<th>$\beta$</th>
<th>$\epsilon$</th>
<th>Simulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Case 1</td>
<td>2000</td>
<td>200</td>
<td>3</td>
<td>0.02</td>
<td>5</td>
<td>0.008</td>
<td>Figure 2</td>
</tr>
<tr>
<td>Case 2</td>
<td>2000</td>
<td>200</td>
<td>3</td>
<td>0.02</td>
<td>5</td>
<td>0.03</td>
<td>Figure 3</td>
</tr>
<tr>
<td>Case 3</td>
<td>2000</td>
<td>600</td>
<td>3</td>
<td>0.02</td>
<td>5</td>
<td>0.008</td>
<td>Figure 4</td>
</tr>
<tr>
<td>Case 4</td>
<td>2000</td>
<td>600</td>
<td>5</td>
<td>0.02</td>
<td>3</td>
<td>0.008</td>
<td>Figure 5</td>
</tr>
</tbody>
</table>
to privacy and information disclosure are more prolonged compared with Case 1, and the rate of infected citizens who prefer privacy will finally overcome the rate of uninfected citizens who prioritise information disclosure.

In Case 3, the number of infected citizens who preferred privacy with Qinfect increased from 200 to 600. The ratio of uninfected citizens who choose information disclosure to infected citizens who prefer privacy changes from 10:1 to 10:3. The simulation of Case 3 is shown in Figure 4. It is found that the cyclical shifts in psychological behaviour related to privacy and information disclosure in Case 3 are relatively more prolonged than in Case 1. Additionally, the highest expectation for the rate of uninfected citizens supporting information disclosure and the rate of infected citizens preferring privacy in Case 3 is more significant than in Case 1.

Case 4 further sets the growth rate of uninfected citizens who support information disclosure $\alpha$ from 3 to 5 and sets the decreasing rate of infected citizens who prefer privacy $\beta$ from 5 to 3. The simulation of Case 4 is shown in Figure 5. It is found that the cyclical shifts in psychological behaviour related to privacy and information disclosure in Case 4 are longer than in Case 3. In contrast, the
highest expectation for the rate of uninfected citizens who support information disclosure and the rate of infected citizens that prefer privacy in Case 4 is restrained compared to Case 3.

**CONCLUSION**

The practice of data utilisation and personal information protection during the epidemic provides a new observation perspective for improving the private information protection system. At present, the data management system is constantly improving and becoming more effective. Finding a balance between public health and personal information protection should take the balance principle from the abstract and empty basic principle. Then, it develops into a new and specific, operable specification.

**Dynamic Balance Between Privacy and Information Disclosure**

In recent years, the government has actively promoted the legislation and practice of personal information protection. The private information protection system has been continuously improved, and
law enforcement has been significantly strengthened in critical areas. Although information protection is vital in the digital economy era, data utilisation is a powerful driving force for the development and progress of all fields of society, in which a delicate balance must be maintained. Due to the need to protect public health and infectious disease prevention and control, personal information can be collected and used at will. Generally, information related to health conditions belong to the scope of the right to privacy. No unit or individual has the right to disclose private information without the patient’s disclosure or consent. However, infectious diseases are not simple personal diseases but rather are closely related to public health. Suppose the identity, address, contact information, whereabouts, or residence of patients with infectious diseases are not known in time. In that case, it is impossible to carry out effective monitoring and forecasting, conduct the corresponding isolation observation and treatment; neither is it possible to effectively cut off the transmission route of infectious diseases or carry out the investigations and research needed for the prevention and control of infectious diseases. Therefore, the autonomy of personal information of patients with contagious diseases should be somewhat limited. Moreover, this restriction also extends to pathogenic carriers, suspected infectious disease patients, and close contacts. The primary expression of the condition is the obligation to provide relevant information.

However, there must be boundaries for the violation of personal information autonomy for reasons of public health and the prevention and treatment of infectious diseases. After all, even if the vast majority of people agree with the legitimacy of restrictions, they must be worried that in case they, unfortunately, become a patient, pathogen carrier, suspected patient, or close contact, the truthful reporting of personal information to the public health department and the exposure of information that may occur with it will result in embarrassment, insults or discrimination. Moreover, such disclosure carries unexpected obstacles, especially in social interaction, work and employment, medical insurance, and other aspects. In response to this concern, it is necessary to impose the required “reverse restrictions” on the public authorities that collect, use and store personal information to protect individuals who sacrifice personal information autonomy for public health and for public health from overburdening them.

The multiple-choice questions combine various factors to measure value and pursue a balance in the interests of all parties (Zhang, 2013). Therefore, relevant departments should carry out balance testing in the formulation and implementation of norms, consider factors such as the sensitivity of personal information, the recoverability of private rights and interests, and the importance and urgency of public needs, and address the “broad” and “strict” relationship of data management.

Specify Regulations of Information Disclosure to Public in COVID-19

Personal information obtained from mobile phone signalling analysis, such as individual tracking, geographical location, home address, work unit, and other factors closely related to the movement of people, contact network, family members, identity information necessary for contact tracing, and medical information, may become the object of epidemic prevention and control under specific circumstances. Under what circumstances will the relevant information provided by individuals to their carriers through the use of mobile phones be fully collected, recorded, or even disclosed as a basis for their own and public risk assessment? It is urgent to clarify the data utilisation rules in scenarios such as public events in regulations.

From the perspective of epidemic prevention and control, it is necessary to monitor and master the flow of people across the country and in critical areas through large-level extensive data analysis, conduct situation research and analysis, prediction and early warning, and help improve the refinement and accuracy in policy implementation. In the case of people who are judged to have substantive risks at different levels, it is necessary to identify them and take measures according to the level of classification. In the first case, in people’s information processing, the anonymisation of personal information, commonly known as data desensitisation, is emphasised for overall situation research
and analysis only. The use of personal information with substantial risks in the second case involves restoring, tracking, and processing original personal data based on risk assessment.

Different utilisation rules, identification standards, protection measures, management systems, and subject responsibilities can be considered according to the different levels of data identification, such as anonymity, relevance, and identifiability, combined with the sensitivity and importance of data and the urgency of public needs. Policy-makers should continue to issue guidance examples to explain the specific meaning of national interests and public interests in cases and different industry backgrounds, clarify the reasonable boundaries between personal information rights and general needs, law enforcement assistance, academic research, and other legal protection reasons, and provide clear guidelines and reasonable expectations for the balance of data utilisation and protection.

This research develops a framework to reconcile the conflict between privacy rights and information disclosure in response to COVID-19. It supports customer relationship management of companies in digital governance by coordinating the private and public interest in data use based on incentive compatibility by the specified boundary of information disclosure. Volterra differential equations have been applied to simulate the dynamic context in the psychological behaviour of preferences for privacy and information disclosure. Digital governance in privacy and information disclosure is essential to global companies involved in customer relationship management in the Chinese market. It also helps global managers further understand the dynamic context of corporate leadership in digital governance in response to COVID-19 in the global market.
REFERENCES


Yinghui Cai is an Associate Professor of Law, PhD in CUPL, Visiting Scholar at School of Law, Northwestern University (USA). Assistant Director of the Institute of International Dispute Prevention and Settlement (IIDPS), Master’s Tutor.

Xiaotao Zhang is the dean of School of International Trade and Economics, Central University of Finance and Economics. His areas of research include international trade theory and policy, foreign direct investment (FDI), and multinational corporation management.

Niu Huayong, PhD and professor of Economics, is the dean of International Business School of Beijing Foreign Studies University (BFSU), and a member of the Teaching Steering Committee for Master’s Degree in International Business of the Ministry of Education. He also served as the executive director of the Society of Management Science of China (the director of Industrial Finance Management Committee), the executive director of Chinese Academy of Management (the director of International Business Negotiation Committee).

Wei Li, PHD in Law, major in procedure law, human rights, corporate compliance.

Da Huo is a professor at School of International Trade and Economics at Central University, and has publications in Technological Forecasting and Social Change, Frontiers in Public Health, Economic Research-Ekonomska Istrazivanja, with focused research in international business area.

Jianing He, PHD, Management Science and Engineering, South China University of Technology.

Hong Chen, School of International Economics and Trade, Central University of Finance and Economics.