Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSR

Computer Law & Security Review

Analysis of the attributes of rights to inferred information and China's choice of legal regulation

Fei Feng[a], *Xia Wang*[b,*], *Tianxiang Chen*[c]

[a] *Institute for Chinese Legal Modernization Studies, law School of Nanjing Normal University, Collaborative Innovation Center for Regional Rule of Law in Jiangsu, No.1 Wenyuan Road, Nanjing 210023, China*
[b] *School of Intellectual Property of Nanjing University of Science & Technology, Intellectual Property Development Research Center of Jiangsu Province, No.200 Xiaolingwei Street, Nanjing 210094, China*
[c] *law School of Zhejiang University, No.51 Zhijiang Road, Hangzhou 310008, China*

ARTICLE INFO

Keywords:
Inferred information
Right to personal information
Right to privacy
Intellectual property
Legal regulation

ABSTRACT

Researchers who study data collection, analysis, and use in the era of big data and algorithms are paying increased attention to inferred uses. The information inferred by an algorithm has distinct personality and property interests and challenges existing theories of personal information and privacy. However, a complete method of legal regulation for such information does not yet exist in China. This article focuses on how to recognize the nature of inferred information and how to carry out appropriate legal evaluation and regulation to better protect the legitimate rights and interests of relevant subjects in China. Based on China's social needs and judicial practice experience, the "contextual integrity" privacy theory developed by Professor Nissenbaum can be used to evaluate whether inferred information is infringed upon, and we believe that China is likely to adopt the US regulatory model.

1. Introduction

Data are of immeasurable value, and data can speak: "As long as we torture data, it will confess everything".[1] How to make data "speak" can be understood in two ways: on the one hand, such "speaking" comes from the self-presentation of the data, but on the other hand, understanding this "speaking" depends primarily on the deduction and prediction of the data or information. We can conduct data analysis through the mathematical mechanisms of big data and algorithms, explore the correlations among data, establish a predictive model, and thus infer certain valuable information. "Inferred information" is a new type of predictive information formed from the original data or information through data analysis technology. The core idea of the era of big data is not entirely that information should be accurate but rather that it should be predictable. Inferred information is not a science fiction story. Economists have long pointed out that observable characteristics such as privacy and discrimination in statistical data are related to unobservable characteristics (such as worker productivity and willingness to stay in the labor market), and employers will use the latter as their "agents" to take improper actions.[2] Psychologists have used psychological portraits to infer mental activities and characteristics and further speculate on possible behaviors and actions based on these inferences. Medical researchers can obtain additional information from limited data.[3] Collected personal information can easily reveal the true appearance and living environment of a person through big data analysis and data mining. In the field of justice, Posner put forward "attitude theory" regarding judicial behavior.[4] The development of "ubiquitous computing" has made infor-

* Corresponding author.
E-mail addresses: fengfeimail@126.com (F. Feng), gracewong1507@hotmail.com (X. Wang), 3539702316@qq.com (T. Chen).

https://doi.org/10.1016/j.clsr.2021.105565
0267-3649

mation technology researchers pay increasing attention to information collection. Ubiquitous computing devices can easily infer a person's behavior patterns and other situations from different information collected.[5] For example, a survey by a Dutch privacy protection agency pointed out that a smart running shoe from Nike connected data about a user's physical activity to the user's smartphone or watch device, and those data were eventually collected by the manufacturer. This processing of user health data is risky and may result in discrimination based on personal assumptions or actual health conditions.[6] Big data and algorithms can infer the education level, intelligence, and cognitive ability of individuals by analyzing the keywords they use and pages they visit[7] and can even infer job applicants' race from their names. Therefore, many new technological problems in the era of big data and artificial intelligence[8] can be reduced to the problem of information inference and inferred information.

In China, with the development of information technology, people are increasingly using inferred information. For example, online advertisers will comprehensively and accurately analyze the user information they have obtained, and based on the results of such analysis, place advertisements targeting specific consumers to realize the precise marketing of a product. Some websites continuously adopt new technologies to track and record users' online behaviors and infer additional information. This conforms to "mosaic theory", which posits that seemingly insignificant bits of aggregated information may create a fine-grained picture that can threaten privacy.[9] Therefore, the development of inferred information technology has threatened the protection of privacy in network information in China. These realistic challenges have also prompted us to consider the following questions: How do we recognize and identify inferred information? How can we prevent the infringement of inferred information? Currently, there are four different views on the nature of rights to inferred information: personal information rights theory, privacy rights theory, intellectual property rights theory, and compound rights theory. Different viewpoints result in different legal protection models. Regarding the overall situation of relevant legislative practices, the General Data Protection Regulation (GDPR)[10] of the European Union adopts a basic rights model to protect the rights to personal information. Although the United States recognizes the right to privacy as a basic right, issues related to personal information are included in the privacy framework to protect the privacy and negative freedom of personal information. Other countries also have corresponding laws and regulations, but they have largely failed to effectively regulate inferred information, and there is still much room for improvement.

To regulate inferred information legally, we must solve the problem of evaluation—that is, how to evaluate whether the inferred information and the inferred behavior are illegal. After analysis, we believe that the framework of the contextual integrity theory proposed by Professor Nissenbaum of the United States can be used as a theoretical basis and method for considering privacy and evaluating whether inferred information is infringed, which is beneficial to the regulation of inferred information in China. In China, when regulating and protecting speculative information, the relevant authorities must also respect privacy and protect digital human rights in the process of regulating and protecting inferred information.

To analyze the nature of the right to inferred information and the legal regulations of inferred information in China, this article primarily adopts the research methods of logical analysis, comparative analysis and case analysis.

1.1. *What is inferred information?*

Based on the source and generation of data, we can divide them into "collected data/information" and "inferred data/information". The former category includes metadata and information, which means data that are directly collected without any processing; the latter category is data/information produced by secondary mining, analysis and processing using big data and algorithms based on a plurality of original data with potential connections. Many scholars have proposed similar concepts of data classification. For example, some have proposed "data derivatives" and "processed data".[11] The World Economic Forum (WEF) and ICO also distinguish between inferred data and derived data,[12] as do other organizations.[13] In addition, there are many concepts similar to inferred information. For example, profiles are associated with three main types of inferred information: (1) profiles as inferred data,[14] (2) profiles based on inferred data,[15] and (3) profiles that create inferred data.[16] The inferred information is analyzed from different angles. At present, scholars in China have not discussed inferred information as deeply as scholars abroad have. They pay more attention to data derivatives and the nature of rights,[17] which can actually be regarded as an analysis of inferred information.

In fact, people's understanding of the concept of data does not stop at the original data themselves. The collected data are, of course, important; however, the value of the data lies more in their "use",[18] which is not limited to the "adoption" we usually understand but often takes the form of a "secondary use",[19] that is, speculative usage. The main purpose of collecting information is to obtain "useful information that is very similar to knowledge". Information collectors must often attempt to draw inferences from the original information collected. According to these inferences, they can take corresponding actions and establish contacts.[20] In reality, we often find that even when companies or organizations cannot directly collect the personal data they want to obtain, they can nevertheless make inferences from other data, and the accuracy of these inferences is often very high.[21] Therefore, the concept of inferred information refers directly to the actual operation of personal information in the era of big data, which means that through the use of big data and algorithms, hidden information can be inferred from explicit information, and relatively direct information can be inferred from indirect information; the complete (integrated) information panorama can be inferred from incomplete (integrated) information fragments; sensitive information can be inferred from nonsensitive information; relevant information can be inferred from irrelevant information; illegal information can be inferred from legal information; nonpublic information can be inferred from public information; and so on.

Strictly speaking, information is not the same as data. Considering that big data are open to all data, the algorithm

mechanism that is used to infer breaks the barriers of metadata, data, information and knowledge.[22] Thus, it seems that the distinction between the content and form of information and data does not make much sense.[23] There is no strict dichotomy between data and information; rather, there is a spectrum, and a datum will move along the spectrum of informational value according to added information, deductions, and inferences.[24] It is necessary to understand the contextual elements of the richness of data, the intention of the data controller and the applications in the present and future.[25] Instead of considering the data and information themselves (whether they are personal data or not), it is better to consider the risks identified in a specific process and the risks of harm to individuals (i.e., inferred risks) as well as the possible severity of any damage. The treatment process should take measures according to the risks.[26]

In reality and our existing knowledge, the boundaries of the process of inferring information and the method of collecting information are unclear. Sometimes inferring information is also regarded as a method of collecting information. The collected information is used for inference, and information is further collected through inference.[27] As a result, we often cannot distinguish whether the data are sensitive, public, or complete, which is the basis of privacy protection. Any data can be sensitive because they can be inferred from sensitive information. Even if the inferred information is not sensitive, the information is gathered by inference rather than consent, and the process itself is still sensitive. Therefore, it is believed that the concept of inferred information was first proposed based on the use of information rather than on the subject of the information. This situation necessitates analyzing the attributes of the right to inferred information and its regulation.

1.2. *How is inferred information produced?*

In the era of big data, it is not impossible for people to discover related relationships or even "predict the future" using the scientific and technological rationality of big data and algorithms. The core value of big data lies in "predicting the future".[28] IBM summarizes the characteristics of big data as "5 Vs": volume, velocity, variety, value and veracity. However, big data also includes a sixth "V", valence, which refers to how big data is related. Therefore, big data can also refer to a methodological concept; that is, big data can objectively and accurately discover the correlation between truth and things that have no logical connection.[29]

Inferred information is based on big data, algorithms, and artificial intelligence (machine learning). Human activities, in the information age, generate massive data information in people's work and lives. These forms of data include machine-generated structured data (such as cash receipts), human-generated unstructured data (such as various review texts and photographs on social networking sites and shopping websites), and mixed data generated by organizations (various data, including the previous two). We can observe both microscopic changes in human tissues and all interactions among millions of people through big data. When observing fine-grained interaction patterns within an organization, people can rely on customized organization or individual performance and predict how individuals will respond to new situations.[30] The working principle of big data is based on prediction science and evidence-based methods represented by applied mathematics, statistical technology, and computer science, and the main goal of big data analysis is to optimize or select the best available variables.[31] In other words, the data contain a "rule" or relationship, and big data can thus be used to collect, analyze, and mine related relationships among data and build prediction models for a set of discovered and useful relationships. These models can classify behaviors and evaluate the probability of specific behaviors occurring or the characteristics of specific individuals or groups under given conditions (e.g., using mathematical tools such as Bayes' theorem). Moreover, "supervised machine learning" can continuously add inferred information and models to the database as a way to collect information to continue learning and improving the model. This approach has formed a nearly perfect recursion, or closed loop, of "collection-modeling-speculation-learning-modeling" to change the operation of an existing system in relation to the desired target.

The "basic model"[32] of inferred information is represented in Fig. 1:

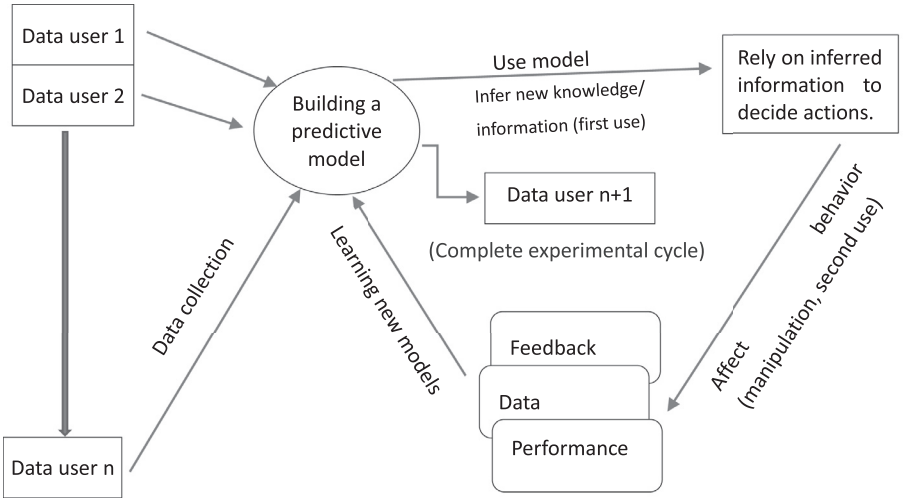
1.3. *Characteristics of inferred information*

Big data and algorithms make decisions based entirely on correlations; that is, "data analysis and mining is a model for discovering or inferring unknown facts in big databases. It does not rely on causality but relies on correlation for prediction and inference, the newly discovered information is non-intuitive, unpredictable, and the entire process is quite opaque."[33] The black box operation of big data, which is inherently acontextual, syntactic, algorithmic, empirical, and deterministic, cannot even explain itself.[34] When the data analysis reaches a certain level, qualitative change or even alienation will occur, and personal behavior patterns will then become transparent, calculatable and predictable.

This discussion shows that inferred information has an important characteristic; that is, it is possible to speculate about a certain factual state of the data subject, which means that inferred information is not as deterministic as other information—it presupposes the existence of a certain state or fact. Although the existence of this state or fact is highly probable, it has not been directly proven and cannot be included in personal information until the information is used and the information subject is confirmed (or other proof is provided). This characteristic is particularly reflected in certain speculations about personal interests, habits and personality. "Big data space" is a "timespace" that can synchronize data exchange and parallel processing, challenging the traditional concept of time (past and future).[35] More importantly, regardless of the authenticity of the information content, the information has the potential to impact and threaten the traditional concepts of personal privacy and autonomy in this sense.

2. The nature of rights to inferred information

Personality, property and social interests contained in information provide a legitimate basis for the object of legal rela-



tions in the data age. However, there are divergent opinions on the nature of rights to inferred information. Different theoretical viewpoints have resulted in different understandings and regulation strategies.

2.1. *Personal information*

This theory focuses on the data source and content of inferred information, regards inferred information as a part of personal information, and emphasizes the right to the personal ownership and active self-determination of inferred information. So-called personal information refers to an identifiable symbol system that is associated with a specific individual and reflects individual characteristics, including personal identity, work, family, property, health, and other information. "Identification" refers to the process of locating an entity in a specific crowd or environment and is usually carried out through identity proofing. It means that an individual can be "recognized" through personal information and refers to identification in a broad sense; that is, as long as this information has a certain connection with the personality or identity of an individual, it can be considered part of identity.[36] From a practical point of view, China, the European Union and the United States have all emphasized identity in the concept of personal information in their relevant laws and regulations.[37] Therefore, this view holds that not only does the inferred information use collected personal information as the source material or raw material but also that the information inferred through processing analysis often points directly to individuals, although there is no complete coincidence between the inferred information and actual personal information. Considering the source and direction of the information, it is generally believed that inferred information should be a part of the right to personal information. Therefore, inferred information is considered to be a type of personal information that cannot be regarded solely as a new type of data but instead should belong to the category of personal information[38] and may even be classified as personal private property.

There is no doubt that inferred information is also identifiable, as it is obtained from the analysis of various items of personal information. Therefore, inferred information is often attributed to personal information in theory and practice,[39] and the right to inferred information is considered to be a type of personal information right, as individuals have the right to self-determination.

However, this view faces both theoretical gaps and practical difficulties. First, in accordance with the strict idea of protecting the right to personal information, if the inferred information is acknowledged as personal information, it will inevitably lead to the unlimited expansion of the content of personal information. In the existing theoretical explanations of the right to personal information, such information does not contain meaningless data. It is also necessary to recognize these meaningless data—indeed, any data because they can form the source of inferred information directed at individuals—if inferred information is generally considered personal information. Therefore, it is overly simplistic to use one factor to identify personal information,[40] and the theory of the right to personal information and the regulatory model based on this theory will also encounter difficulties. Second, the basic connotation of the right to personal information (self-determination) is the subject's complete (strict) self-determination of information. However, it is quite difficult for data subjects to realize the autonomous control of their personal information, not to mention the control of inferred information. Big data technology constantly collects data, online and offline, and most of the collected data are integrated in a multinational cloud storage method. In addition, the nature of data mining is predictive, but the prediction process is difficult to decipher, and the prediction content is unknown.[41] Companies and governments will evaluate and provide services to individuals based on this inferred and possibly incomplete information, so individuals will not even be able to determine what information is known by others and what judgments are formed.[42]

Professors Sandra Wachter and Brent Mittelstadt put forward a so-called new right to inferred information, that is, the right to reasonable inferences, to help close the accountability gap currently posed by high-risk inferences, meaning inferences drawn through big data analytics that are privacy-invasive, reputation-damaging, or have low verifiability in the sense of being predictive or opinion based while being used

for important decisions.[43] The new right also emphasizes personal control and choice and still belongs to the personal information right. It can be extended to the personal information rights system by explaining the existing legal concepts, subjects' rights and controllers' obligations.

2.2. *Privacy*

A similar view to the right to personal information is the attribution of the inferred information to the right to privacy. This view highlights the sensitive components of inferred information, focuses on the benefits of its personal nature (privacy and autonomy), and places privacy at the center of the discussion rather than treating it as merely one of many interests involved in inferred information. The privacy viewpoint is reflected in the discussions of many scholars. For example, some scholars have argued that the privacy model is the main legal regulation method when discussing the risks associated with the automatic completion function of search engines.[44] Other scholars have adopted the idea of privacy when discussing the issue of personal credit benefits.[45] In fact, both the automatic completion of search engines and the collection and prejudgment of personal credit information involve inferred information. For example, in the case "United States v. Wurie", the judge identified the inferred information that may be generated by collected mobile phone information as private content.[46] Many computer scientists have also focused on how to reduce privacy risks rather than on ensuring information self-determination.[47]

Many practical examples to support the privacy viewpoint can be found in real life. For example, shopping websites and social networking platforms often record and track search keywords according to what a user clicks and browses and then push related service information and advertisements to the user. These pushes often accurately "predict" the user's recent concerns and provide "personalized services", but the convenience comes at the cost of snooping or even violating personal privacy and preferences. As another example, Tesla uses cookies, pixel tags, analytical tools and other technologies to collect various types of data and metadata, including contact information, browsing history, navigation history, and broadcast listening history, which can be used to infer and provide convenient personalized services.[48] Some "predatory advertisements" use inferred information to target those who are "vulnerable" and in "painful" situations, such as women who lack self-esteem, hold low-paying jobs or are pregnant, and promote related products to add their "anxiety".[49] Faced with these social phenomena, privacy theory provides a set of stricter regulations and normative strategies than the right to personal information.

However, there are two problems with privacy theory.

First, although it is born of personal information, privacy theory does not completely transcend and overcome the shortcomings of the theory of the right to personal information. The content of privacy is extensive, including free thinking; personal solitude; not being monitored, searched and interrogated; personal reputation; and the control of personal information.[50] However, information privacy is a nonabsolute moral right in a normative sense; that is, people have the right to obtain, directly or indirectly, information about themselves; others can obtain information about themselves; and technology can be used to generate, process or disseminate information about them.[51] Therefore, the boundary between privacy and personal information is often unclear.

Second, regarding inferred information as contained within the right to privacy has certain limitations. Privacy does not protect data that do not have a clear privacy benefit, but inferred information is often obtained through the analysis of such information without privacy characteristics, which makes it impossible for privacy theory to cover all the interests of inferred information.

Take metadata as an example. From the perspective of privacy, metadata are meaningless and nonsensitive data, and the collection of metadata does not infringe on personal privacy. However, in real situations involving inferred information, metadata play a vital function of information organization, which allows data to be easily read and processed by machines and helps produce high-quality, personalized search results.[52] As a result, many scholars have changed their attitude towards metadata protection.[53] Because the rapid progress of algorithms and the occurrence of inferred information in the era of big data have made metadata meaningful, if we nonetheless insist on the theory of privacy, the real needs of inferred information protection cannot be satisfied.

From this point of view, personal information differs from private information, and inferred information has the double attributes of personal information and private information.

2.3. *Intellectual property*

If the theory of the right to personal information and the right to privacy are perspectives on the allocation of rights and interests based on the origin of inferred information, the theory of intellectual property is another point of view generated from the actual production process of inferred information. From the perspective of intellectual property, on the one hand, the software or algorithm that creates, stores, and mines data is a kind of intellectual property, and inferred information is a derivative product of this intellectual property that is different from the information originally collected. It is "new information" generated by big data and algorithms through deep learning and is separate from the information source. The accuracy of the inferred information originates from the rationality and scientific accuracy of the algorithm; as a result, the labor of the algorithm writer determines the reliability of the inferred information. On the other hand, although the inferred information is automatically generated by the algorithm, its content still needs to be interpreted by the algorithm writer. The storage of inferred information also depends on the investments of technical staff and technology companies: data analysis requires not only labor but also the establishment of databases to condense the intellectual labor and economic input.[54] Therefore, inferred information should be included in the "intellectual property" of data parsers based on the justification of intellectual property and protecting the legitimate interests of scientific and technological personnel and enterprises.

The theory of intellectual property has also gained a certain degree of recognition in practice. For example, in the case "Search King v. Google",[55] the judge considered the company's

algorithm (and its results, that is, inferred information) to be a subjective opinion and thus protected free speech. The subsequent cases "Landon v. Google"[56] and "Zhang v. Baidu"[57] both followed precedents, and both acknowledged that algorithms are free speech without exception. Although many scholars have criticized this statement,[58] according to this view, algorithms are regarded as corporate property, and the information inferred, which is regarded as an expression or subjective opinion of the enterprise algorithms, should be protected as the intellectual property of the enterprise—at least theoretically.[59] The theory of intellectual property provides a broader legal space for data analysis activities and plays a powerful boosting role in stimulating the vitality of network science and the technology and information market.

However, the theory of intellectual property still faces many challenges in theory and practice.

First, although the intellectual work of data analysts is condensed in the process of generating inferred information, we can use the rules of addition and processing in property law to endow processors with property rights to new products with value that obviously exceeds the value of the raw materials. Inferred information content has distinct personal property and personality interests that differentiate it from ordinary property. We cannot ignore such distinctions. Moreover, owing to the social attributes reflected in the substantial inferred information about individuals, the state and society have special interest demands for this information.

Second, even if the algorithms and software that create, store, and mine data are recognized as intellectual property, it does not necessarily follow that the data (inferred information) themselves must be protected as intellectual property. Instead, they can be treated as trade secrets, which will continue to stimulate the development of the science and technology industry.[60] Intellectual property theory is not the only option for stimulating innovation.

Third, regarding inferred information as the intellectual property of data analysts will likely lead to endless data collection and information speculation by scientific and technological enterprises. Abuse of information technology and algorithms will lead to malicious use of inferred information for profit and may even threaten the value of human beings as subjects. Although the intellectual property approach can effectively promote the expansion of production in the field of information, it is still impossible to determine the value of human beings as subjects.

2.4. *Compound rights*

The above three theories are not only descriptions of academic viewpoints but also analyses of practices. Different ways of imagining individuals, data, and the relationship between individuals and data produce seemingly different discourse systems. Careful consideration reveals that these discourses often overlap. The right to the self-determination of personal information also means that individuals are treated as private consumers and can trade their own data freely. The data analysis subject treats data as personal assets, which also reflects personal self-determination. In addition, both the right to positive personal information and the right to negative privacy may be basic rights that overlap, so it is difficult to separate them to discuss inferred information. It is difficult for us to fully attribute inferred information to a single type of right because multiple forms of interest are involved. Therefore, compound rights theory is produced in an effort to decompose and categorize inferred information into different types of rights. Professor Nissenbaum's concept of "contextual integrity" is a typical compound rights theory of inferred information. When she discussed the issues of knowledge discovery in data (KDD), in-depth data, and data mining, she first acknowledged the real possibility of information inference and the threat to privacy and regarded privacy as a context, with the rights boundaries of inferred information determined according to different contexts.[61] The legal practice of Australian data protection also reflects the theory of compound rights. In this legal practice, consumer rights are the basis of all data rights, individuals are considered privacy consumers, and privacy laws must be market oriented. Furthermore, data are regarded as assets,[62] and individuals have rights to trade their own data.[63] Moreover, data are also considered to be an asset of the data-holding entity. This perspective reflects the views of the right to privacy and the claims of the right to personal information as well as the opinions of intellectual property rights theory.

The theory of compound rights does not truly solve the problem of the rights attributes of inferred information; it only provides an attitude that changes with the situation. The proposition reflects the complexity of reality and the confusion about how to regulate inferred information.

3. Legal regulations of inferred information

Different doctrines of rights attributes reflect the essence of inferred information from different aspects and, when different theories are taken as the dominant viewpoint, result in different legal regulation modes.

3.1. *U.S. industry self-discipline model*

Generally, the United States does not have a written law that predominates in the protection of information privacy. Instead, its privacy protection is an industry self-discipline model. Data protection in the United States is based on the right to privacy as the main framework, laws and regulations are scattered throughout every state and industry, and precedents and statutes are also different. This model is market driven and treats individuals as privacy consumers, participants in market relationships, and traders in goods (personal information).[64] The Consumer Online Privacy Rights Act (COPRA) proposed by Maria Cantwell and other members of Congress in 2019 explicitly included derived data in the scope of protection: “derived data” means covered data that are created by the derivation of information, data, assumptions, or conclusions from facts, evidence, or another source of information or data about an individual, household, or device used by an individual or household. Information derived from publicly available information is not publicly available information.[65] The California Consumer Privacy Act (CCPA) of 2020 is currently the strictest personal information and privacy protection law in the United States. It clearly defines inferred

and inferred information,[66] but the definition is limited to information inferred from personal information. In its 2012 report on data security, "Protecting Consumers' Privacy in a Time of Rapid Change", the Federal Trade Commission (FTC) took data security, reasonable collection limits, sound retention practices and data accuracy as the four key principles of privacy protection. However, the FTC believes that information is static and that controlling the original collected information is sufficient to protect privacy interests, so it does not discuss situations in which additional personal information can be inferred from the collected information, nor does it pay attention to how enterprises should treat the inferred information. Recently, the FTC has realized this problem. The FTC now points out that "data brokers" collect and use not only original data but also data derived from original data and then "classify" data subjects (consumers) through behavior prediction and feature identification.[67] The data industry in the United States and its practitioners resort to technical means to achieve deidentification of personal information, and data controllers make it difficult for data users to identify data subjects by changing or deleting personally identifiable information in datasets.[68] Deidentification of personal information is performed to eliminate the possibility of inference from the source of the data, realize the anonymization of the data, and ensure that the data are no longer identifiable and cannot be used to identify or contact individuals.[69]

3.2. *EU centralized legislation model*

The European Union has adopted a regulatory model of centralized legislation. Here, we mainly focus on and analyze the GDPR, which aims to update all previous EU data protection laws in response to the modern scientific and technological developments represented by algorithms and artificial intelligence. Theoretically, the GDPR is based on the strict right to self-determination of personal information and gives such information the legal status of basic rights to protect relevant personal interests. The GDPR divides personal data types in detail according to the sensitivity of data and clarifies the rights of data subjects and the obligations of data controllers. Although the GDPR does not clearly stipulate what is inferred information,[70] its regulation of inferred information is very strict, providing strong privacy and autonomy protection for information subjects. For example, the GDPR gives data subjects the "right to delete", which is designed to prevent personal information from being used improperly for a second time, i.e., for speculation. Article 9 of the GDPR stipulates that if data processing (i.e., information speculation) can reveal information such as citizens' political views and ethnic inclinations, such processing is prohibited in principle; even if personal data are processed for political purposes, they should be handled strictly and meet the requirements, with few exceptions.[71] Article 22 provides that data subjects have the right to be free from restrictions based solely on automated decisions, thus avoiding similar effects on individuals. This means that it is possible for the identification and analysis of user portraits, as well as online recruitment or online performance evaluations without human intervention, to infringe on privacy and autonomy with the information inferred by algorithms. Therefore, such processes need the legal protection of Article 22. Considering this necessity, the GDPR also stipulates that citizens have the right to interpret; that is, the data subject has the right to require the enterprise to explain how the algorithm works and how it makes automatic decisions. In other words, enterprises must explain how information is inferred by big data and algorithms.

3.3. *Other laws and regulations on inferred information*

The regulations of the European Community once stipulated that when determining whether certain information is identifiable, all methods that may be reasonably used by the information controller or others to identify the person should be considered. Germany's judgment in the 1983 census case stated that there were no unimportant personal data, and because automated data processing could generate partial or even complete personality images,[72] the right to self-determination of inferred information and personal information was confirmed. In 1990, Germany comprehensively revised the Federal Data Protection Law of 1977, enacting the regulation of automatic and manual processing of data, limiting data collection, and prohibiting the processing and use of personal data in principle.[73] Norwegian data protection authorities stipulated similar personal information processing principles, such as the principle of restriction of purpose and the principle of data minimization, in the 2013 report "Big Data Privacy Principles under Pressure". In the 2008 report "Australian Privacy Laws and Practices", the Australian Law Reform Commission suggested that privacy law redefines personal information as information or opinions about an identified or reasonably identified individual, regardless of whether it is true or whether it is recorded in physical form.[74] Similarly, Canada's Personal Information Protection and Electronic Documents Act of 2002 did not define sensitive information but gave organizations the power to determine what sensitive information is. In addition, antidiscrimination laws in other European and American countries, as well as in Taiwan and Hong Kong in China, prohibit unfair treatment based on personal characteristics (such as age, race, gender, and skin color). In cyberspace, these personal characteristics are mainly inferred through big data and algorithms. Therefore, antidiscrimination laws actually regulate inferred information by restricting the purposes of data use. For example, merchants are prohibited from implementing "price discrimination" on the basis of inferred information.

3.4. *Comparison of different regulations*

In general, the GDPR of the European Union adopts a basic rights model to protect personal information, so this model protects personal information and positive freedom more strictly than others. Although the United States also recognizes privacy as a basic right, issues related to personal information are incorporated into a more specific privacy framework to protect personal information privacy and negative freedom. Most laws and regulations of other countries and regions are relatively general and therefore insufficiently specific. The abovementioned various regulations reflect two different regulatory ideas: direct regulation and indirect regulation. The former refers to the protection of private information

through speculative behavior, such as the purpose restriction principle of data processing and the regulation of algorithms, which is a kind of ex ante regulation.[75] The latter refers to the prevention of speculation through regulating information, such as strictly defining personal information, distinguishing and prohibiting the collection of sensitive data, following the informed consent framework, and establishing various data rights. Direct regulation aims to protect the privacy of information, which reflects the theory of the right to privacy of inferred information, while indirect regulation takes the self-determination of personal information as the starting point, which reflects the theory of the right to personal information of inferred information.

As shown by the analysis above, the relevant provisions of the GDPR are ill-equipped to handle the problems of inferred information, while the US industry self-discipline model addresses different areas of privacy.

4. Legal regulation practice and choice of inferred information in China

4.1. *Legal regulation practice of inferred information in China*

A legal system for data protection has not yet been formed in China, and the protection of data information is achieved primarily through department laws and certain normative legal documents, for example, Article 253 of the Criminal Law of the People's Republic of China (PRC)[76]; Articles 111, 1034 and 1035 of the Civil Code of the PRC;[77] Articles 30 and 41 of the Cyber Security Law of the PRC[78]; Article 1 of the Decision of the Standing Committee of the National People's Congress on Strengthening the Protection of Network Information[79]; and Article 9 of the Provisions on the Protection of Personal Information of Telecommunications and Internet Users.[80] China's judicial interpretation also contains provisions on the handling of data infringement and criminal cases, such as "Provisions on Several Issues Concerning the Application of Laws to Trials of Civil Disputes Involving Infringement of Personal Rights and Interests by Information Networks" and "Interpretation of Several Issues Concerning the Application of Law in Handling Criminal Cases of Infringement of Personal Information".[81] Article 18 of the E-commerce Law of the PRC stipulates that if e-commerce operators provide consumers with search results for goods or services based on their interests, hobbies, consumption habits, and other characteristics, other options that do not target their personal characteristics should also be provided, and the legitimate rights and interests of consumers should be respected and equally protected. This provision actually responds to "big data bias", which exposes the real threat of inferred information. One example of such bias is pricing discrimination: for example, more than one client has discovered when trying to book air tickets or hotel rooms through certain online travel agency (OTA) sites that the price is higher for a frequent user of the website than for a newcomer. This discrepancy occurs because companies use information acquired on clients' preferences and purchasing habits to take advantage of them. The "Self-disciplinary Convention on the Collection and Use of Personal Information of Users" (Second Batch), which was passed at the China Internet Conference in 2019, responded to the collection and use of personal information and information inference and stipulated provisions regarding the purposes of restriction. In addition, other departmental regulations have emulated international law, emphasizing the information subject's "consent" and "purpose of use", but the results are still the same as the content of the GDPR mentioned above.

In the case "Ant Financial Services v. Enterprise Search Company", on May 5, 2019, the news that a famous small online loan company in China had begun to liquidate caused a sensation in the industry. The Enterprise Search Company pushed the news to its subscribers through in-station messages, daily monitoring reports on the "Radar Monitoring" service, mail, etc., claiming that the small loan company Ant Microloan, which belongs to Ant Financial Services, had begun to liquidate and listing the risk level of this news as "warning information". The information quickly spread. There were tens of millions of news reports and analytical articles on the theme of "Ant Microloan liquidation" in major search engines, which caused panic in the market and among users. Ant Financial Services therefore sued Enterprise Search Company.

According to China's "Information Security Technology and Personal Information Security Regulations" (ISTPIS), user portraits are processes of forming personal characteristic models by collecting, aggregating and analyzing personal information and analyzing or predicting the personal characteristics of a specific natural person, such as occupation, economic status, health, education, personal preferences, credit, and behavior. In the case above, the Hangzhou Internet Court held that the defendant automatically monitored the enterprise information that concerns users, collected and processed these data and other free public data, and pushed out early-warning information. Moreover, this inferred information was erroneous and distorted, which greatly misled the public.[82] Although the ISTPIS list various categories of sensitive personal information, including property information, health and physiological information, biometric information, identity information, network identity information and other information, metadata continue to be ignored. The identification of sensitive information in China's judicial practice generally considers personal safety and property security, as it is extremely easy for such information to lead to theft, fraud, extortion and related crimes after being illegally obtained, sold or provided. This kind of information has the potential for greater social harm,[83] such as tracked information.

In the case "Mr. Liu v. Today's Headline", the plaintiff, Mr. Liu, found that after he replaced his mobile phone on January 29, 2018, even though he refused to provide permission to access his address book, the Today's Headline app could still recommend friends from his address book in the old phone. In February 2018, Mr. Liu stated that he believed that the Today's Headline app had not stated that it would collect users' personal information in its "User Agreement and Privacy Terms" but had uploaded and saved his address book without authorization, which seriously infringed on his privacy; thus, he sued the operator of the app in the Haidian court in Beijing. Mr. Liu believed that address book information, as an extremely sensitive type of personal information, is very important to personal safety, property security, etc.

and involves personal social relations, family situations and even business secrets. Uploading and saving such data without permission is a serious infringement of personal privacy. However, the defendant's agent pointed out that telephone numbers play an important role in daily private communications. Telephone numbers should not be kept confidential but must be announced to others. Although an address book contains information such as personal names and phone numbers, the information is not Mr. Liu's own personal information but the information of members of his social network, so it does not belong to the category of Mr. Liu's "private information."

This understanding of sensitive information obviously ignores inferred information and information context. For many app developers, reading personal address books is normal. Address book information has become a source of illegal collection and use of personal information; some developers use this information to engage in telecommunications fraud, violent collection, extortion, and illegal collection of online loans.[84] These activities have already infringed on citizens' privacy because public information also has privacy value, as it can be used for analysis and inference, thus breaking the original context of data flow.

For example, in the first case of "data and trade secret" litigation in China (Jinfeng Technology Co. v. Chen Guoling, Chen Zhiping, Shenzhen Oruifeng Technology Co., and Abbey Mould Engineering Co.), the court of first instance held that emails sent to and from customers and preserved by Oruifeng included the customers' names, addresses, and contact information as well as their trading habits, payment methods and special requirements for products, constituting in-depth information. This customer information is not known to the general public and is not easily accessible. In addition, the value of the abovementioned customer list management information is reflected in the increase in trading opportunities, sales channels, and sales profits associated with it, which can also bring real economic benefits; thus, it has the unique value of business secrets.[85] The Retrial Court held that on the whole, mastering customers' business information, such as contact information, product requirements, and transaction habits reflected in the relevant emails, will inevitably result in enhanced accuracy in finding customers, convenience in establishing contact with business leaders and a competitive advantage in quotation.[86]

The definition of personal information in Article 1034 of the Civil Code of the PRC that was implemented in 2021 has expanded the scope of personal information, which has promoted the protection of personal information and privacy in China to a certain extent.

Generally, China's current legal provisions for protecting data and information are focused mainly on how to prevent others from collecting data and how to safeguard individuals' rights after their data information is infringed. However, there are no provisions regarding the application of data, such as collection, storage, processing, transaction, use, and circulation. It is even more impossible to discuss the use and protection of inferred information, with the result that inferred data information cannot be effectively regulated and protected by law.

4.2. *China's choice of legal regulation on inferred information*

At present, China has not formed a complete scientific understanding of the legal regulation of inferred information. Legal regulation must not only consider the benefits of big data but also balance the harm to privacy caused by big data. Specificity in different cultural contexts also needs to be considered. The United States and the European Union have different attitudes, and not all countries value the active protection of privacy.[87] Even in the same context, the interests of different individuals in privacy and autonomy and the willingness to share information must be considered in real life.

The understanding and protection of inferred information and even personal information in the legal theories and practices of the United States and the European Union are based on different social imaginations of society and individuals.[88] For China, how can this social imagination be used to deal with the problem of information privacy? The preceding analysis reflects that China's Internet technology is developing very rapidly, and the situation China faces is complicated. The privacy protection practices of the United States provide a fairer and more comprehensive protection of privacy and inferred information than those of other countries. The protection model in the United States is based on the contextual integrity privacy theory proposed by Professor Helen Nissenbaum. Based on this theory, the principle of "Respect for Contexts" was put forward in the Consumer Privacy Act of 2012. As a guide, the protection of privacy and inferred information has focused on different fields.

4.2.1. *Contextual integrity theory*

According to this theory, privacy is determined not only by the type of information but also by the context in which the information is collected.[89] "Context" refers to "structured social settings",[90] which is an abstract reference to various social structures that everyone may experience in daily life. Professor Nissenbaum tends to explain context here as social context. She does not agree to define context directly in spatial terms because context is composed mainly of roles, purposes, activities and information types.[91] Specific contexts can be represented as specific spaces, including schools, hospitals, and companies. They have value, and these values are expressed through permitting activities,[92] so they are normative and connect the context to the norm. Since people's activities occur in a variety of different social contexts (situations) and each context has a set of norms that match it and are different from those of other contexts, information privacy should be distributed and protected according to the norms governing specific contexts.[93] Therefore, different contexts should be considered when managing or controlling information; that is, the way of collecting and sharing information needs to meet the expectations reflected in a specific context at that time, and the behavior and practice in a specific context need to follow specific norms.

Information may invade privacy in one context but not in another. For example, in hospitals, doctors can collect medical information about patients, but in workplaces, such in-

formation cannot be collected. Additionally, it is unacceptable for companies to collect large amounts of information from consumers, while it is acceptable for teachers to collect some information from students in schools.[94] This is the principle of appropriateness of norms. Although information needs to adapt to the norms of certain contexts, the theory does not prohibit the cross-situation flow of information. Information collection should consider not only different spaces but also different subjects in specific spaces. For example, the judgment documents of someone who lost a case published on the Internet can be browsed by anyone. Legal professionals and ordinary people may have different attitudes and perspectives on documents, and the information disclosed in the judgment document will also flow to other situations. This is the principle of fluidity of norms. What information can be obtained by police and doctors and how to obtain it are different. Once information is separated from a specific context and placed in another, it will break the contextual integrity.[95] Since the precontext norms are different from the postcontext norms, if the information does not meet one of these sets of norms, privacy invasion will happen. Therefore, information collectors should mine information in their own “divisions” and cannot step into areas that do not belong to them. Information subjects have different privacy demands in different contexts and have the right to respect the context, that is, the right to expect companies to collect, use and disclose personal data in a way consistent with the context in which consumers provide data.[96]

According to the theory, if we want to determine whether privacy has been infringed, we do not need to consider whether certain information is personal or public or whether it occurs in the private or the public domain. The problem lies not in the collection, storage and dissemination of information but in the unevenness of the collection, storage and dissemination of information, such as using the information for a paternalistic and manipulative purpose (e.g., providing personalized services or price discrimination). The information must be placed in a certain context to determine whether it meets the norms of that context and whether it meets the principles of "appropriateness" and "fluidity" of the norms. If the information is valuable in isolation from the context, whether it infringes on privacy cannot be determined. From this perspective, the right to privacy is neither a right to protect private information nor a right to control personal information but a right to the appropriate flow of personal information. When information is transmitted in violation of the two principles of contextual integrity theory, privacy infringement will occur.

Nissenbaum’s theory is more thoughtful than the control theory of privacy and provides a new way to evaluate the technologies and systems that affect the flow of information, answering the questions of when and why privacy issues (especially in the social network environment) occur, that is, why some information is private and why people are dissatisfied with or disregard certain types of information flow. Most importantly, the five variables (five different perspectives) in the theory challenge the understanding of the single element of information privacy, such as whether the information is sensitive, whether the individual agrees with its distribution, the public-private dichotomy of data, and subject control. For example, when people use shopping carts to collect goods in supermarkets and display these goods at checkout counters, the goods will be seen, but this display will not make them feel that their privacy has been infringed. However, if information on the purchased goods is collected or even sold on the website when shopping online, privacy will be infringed. The theory states that privacy norms in a specific situation (or context) involve a variety of different types of information, and the information changes as the context changes. For example, collecting information on marital status is legitimate when men and women are dating but is inappropriate in regard to job interviews. Teachers have unconditional access to the test results of all students but not individual students.

4.2.2. *The development forecast of China’s inferred information legal regulation*

In traditional Chinese culture and social governance activities, it is not that there is no sense of privacy but that there is a complicated contextual structure in the expression of this sense of privacy. On the one hand, this kind of "private" consciousness is always unable to positively resist words from the "public" in the cultural atmosphere and ideology where collective interests are superior to individual interests. Therefore, when an individual’s privacy interests conflict or compete with public interests, the individual’s privacy interests always give way to public interests. Therefore, in the public domain, facing the government authority as the representative of public interests, individuals do not have sufficient discourse advantages and social moral support to advocate their right to personal privacy. For example, in the prevention and control of the COVID epidemic, the government has promoted and applied information technology such as face recognition and health codes on a large scale, which has infringed on citizens’ personal privacy interests to a certain extent. Although many scholars and experts have called for restrictions on the use of these technologies, these voices appear to be very weak against the discourse of protecting public health interests. On the other hand, in social and economic life, the Chinese public is not as "aphasic" as it is in dealing with government authorities when facing the infringement on personal privacy interests by commercial organizations such as Internet platforms. For example, when Tencent Huateng Ma CEO said, "Tencent has data on the faces of Chinese people (voluntarily released) over the past ten years and can even predict what users will look like in old age", it caused a public uproar. In fact, Chinese people do not care about privacy as much as they care about the benefits of privacy. Therefore, when commercial organizations offer certain financial temptations or service convenience as a consideration for exchanging personal information, people often voluntarily abandon personal privacy, although they sometimes are not satisfied with these considerations. Only because they lack an adequate value estimation and sufficient attention to personal information in considering the actual benefits of selling their privacy are people are anxious to voluntarily sell personal information before reading the lengthy and complicated privacy policy. In addition, in the field of personal communication, Chinese people seem to emphasize collectivism, but when facing neighbors, colleagues and even family members, they show a particularly strong sense of privacy protection and can resist the consider-

Data context						
Objective variable					Subjective variable	
Data type	Entity type	Device context	Collection method	Data use	Trust in service providers	Value exchange
What kind of data are involved (financial, medical, location data, etc.)	Who is visiting (government, retailer, enterprise, etc.)	What kind of device is used (mobile phone, tablet computer, etc.)	How data are collected (user provided actively, collected passively, generated automatically, etc.)	How users participate in data use (explicit consent, informed participation, ignorance, automation, etc.)	The relationship between users and service providers	How users view benefiting from their data (perspectives on personal interests and social interests)

ation given by other individuals that is higher than that paid by commercial organizations. Thus, Chinese people's concept of personal information and privacy protection is complex and changes with the context. Studies have revealed that in the right circumstances (defined by social domains, recipients, and purposes), people are quite ready to share information deemed private. However, for information deemed public (defined by its placement in public records), people maintain highly modulated privacy expectations.[97]

When faced with the privacy issues involved in inferred information, the situation is even more complicated. How to prevent the government from interfering too much in citizens' private life through information analysis and how to prevent commercial organizations such as Internet platforms from using information mining technology to infringe on citizens' personal privacy are fundamental issues related to the legal regulation of inferred information. Therefore, it is particularly urgent to strengthen the legal regulation of private information, especially inferred information, in China.

In recent years, influenced by the culture and system of privacy protection in the United States, the Chinese government and legislature have paid increasing attention to personal information and privacy protection. A special chapter of the Civil Code stipulates the legal protection of personal information and privacy, but it stipulates only the rights and interests of personal information and does not specify the rights of personal information.[98] The draft of special legislation on personal information protection also closely follows the international legal trend,[99] which has been submitted to the Standing Committee of the National People's Congress for deliberation. It is expected that it will be formally promulgated in the next two years. Other industries have taken the lead in issuing relevant laws and regulations that fully embody the concept of respecting the context. For example, information inference such as the price being higher for a frequent user of the website than a newcomer is being regulated in tourism and business fields,[100] and the Ministry of Industry and Information Technology has passed special legislation and actions on the governance of personal information collected by apps.[101]

In a typical case, "Pang Lipeng v. Beijing Qunar Information Technology Co." (2017), published by China's Supreme People's Court, in October 2014, after the plaintiff purchased an air ticket from China Eastern Airlines through Qunar, he received a short message regarding suspected fraudulent information related to the purchased air ticket. The plaintiff sued Beijing Qunar Information Technology Co. and China Eastern Airlines Co. for leaking his private information, including his name, phone number and schedule. The court held that Pang Lipeng's name and mobile phone number played an important role in identification and information exchange in daily communications. It seemed to the court that a person's name and mobile phone number should not be kept secret but must be given to others. However, in the era of big data, once individual, isolated, and publicly available personal information is collected, extracted, and integrated, it can be completely matched with a specific individual, thereby forming detailed and accurate overall information on that person. At that time, this comprehensive and systematic overall information is no longer a single item of personal information that can be arbitrarily disclosed. Once overall information is leaked and spread, no one will have their own private space, and personal privacy will be threatened. In this case, the Beijing No. 1 Intermediate People's Court took context as the main consideration and finally determined that a person's name and mobile phone number are private information.[102]

In the case of a user suing Tencent's Wesee for infringement of privacy in 2019, when the plaintiff, Mr. Wang, used a WeChat/QQ account to log in to Tencent's Wesee app, his gender, region, and friend relationship were obtained by Wesee. Mr. Wang believed that Wesee had no right to collect and use the information and that in doing so, it infringed on his privacy and other interests. The judge pointed out that friend relationships in mobile phone address books belong to personal information but not privacy. For privacy and personal information considerations, careful analysis and judgment should be combined with a specific network context. "WeChat friends relationships have reasonable expectations of privacy under certain contexts, but the WeChat friendships claimed by the plaintiff do not include private relationships that they do not want to be known to others, and others cannot judge his personalities which will lead to negative or improper evaluation through his WeChat friendships."[103]

These decisions show that in China's judicial cases, some judges have begun to take context as the main consideration

in judging a case, but there is no consensus in legislation and practice. Therefore, we can say that the legal regulation of private information, especially speculative information, has a theoretical and practical basis in China.

In summary, the theory of contextual integrity has many advantages and can solve many problems regarding inferred information, which provides us with a complete mechanism for evaluating inferred information. Moreover, in China's social environment and judicial practice, the theory has room for survival and development, which could help China cope with many difficult problems involving inferred information in its social development, and this theory could be used to guide China's legislation and judicial practice on inferred information. Therefore, we speculate that in the future, China is likely to adopt the US model in the legal regulation of inferred information.

5. Discussion

When adopting contextual integrity theory and the US regulatory model, China needs to pay attention to the fact that this theory ignores the power of information technology represented by algorithms and artificial intelligence, which is sometimes powerful enough to break or reconstruct the context. It is undeniable that the theory is still an important paradigm for evaluating inferred information because it introduces a new privacy protection mechanism dominated by the concept of context, emphasizing that the rationality of privacy protection should be examined on the basis of the specific environment in which it is situated rather than making abstract prejudgments that deviate from the specific context. Considering the diversity of contexts, the rational use of private information should be judged by integrating various factors. Therefore, we must complement the theory from a technical perspective.

Based on contextual considerations and the refinement of law, we must reconsider the mandatory provisions of existing laws. For China, relevant power subjects must weigh the pros and cons carefully when regulating and protecting inferred information. The power subject must respect privacy and protect digital human rights when formulating relevant legal systems.

Privacy is increasingly becoming an important value in the digital age. While technology provides assistance for privacy protection, it also further threatens privacy (e.g., various network cameras, the pervasive use of unmanned aerial vehicles, the abuse of face recognition by machine learning, and the disclosure of personal information), and the law must adhere to the protection of personal privacy. The characteristics of inferred information and the tyranny associated with government abuse of data and information technology also show that data involve not only memory but also power.

In future legislative and judicial practice in China, it is necessary to link individuals, data and privacy with contexts and to respect individual contexts, data contexts, and privacy as contexts.

Respecting contexts means respect for individuals (preferences), especially individuals (preferences) based on human heterogeneity. The potential of a data-driven economy can be realized only when data can flow and merge to promote new innovative applications. What is important is that these new uses must be consistent with the user's preferences and expectations and win the user's trust by avoiding accidental violation of the context. Context-aware data use is a key factor in achieving the sustainability of this ecosystem.[104]

Respecting contexts also means respect for privacy and other social morality, ethics, and values. The principle of respecting contexts may include and consider many values and purposes, as well as the different values and different purposes of different social contexts, and can assess whether privacy is infringed based on general ethical and political principles, purposes and values in specific contexts.[105] This approach brings balance to many fields of social and political life.[106] When facing the risk regulation of algorithms and artifical intelligence, we must write better values into algorithms and create obedient algorithms; the law must focus on the person who establishes the algorithmic model and abandon unfair algorithmic models.[107] Because of this necessity, respecting contexts can test the morality of the law.[108]

Respecting contexts still requires respect for data and space. Between 2012 and 2013, Microsoft conducted a series of social studies in China, the United States, Canada, Germany, India, Australia, Sweden, and the United Kingdom to reveal psychological attitudes towards privacy protection and legal views on the subject (also reflecting respect for individuals) around the world. The seven variables included in Fig. 2 are collectively referred to as "data context" by the WEF.[109]

Based on these data scenarios, the WEF conducted a series of scientific analyses, emphasizing that data and privacy protection technologies, laws, and policies must respect space and context. The WEF stated that "in today's digital world without borders, people's attitudes and behaviors towards personal data, as well as trust in the digital world, must also establish and consider regional differences."[110] Such consideration is important because contexts are also deeply influenced by different cultural norms (values) in different regions (spaces). Chinese traditional philosophy tends to consider reality a series of relationships (European countries and the United States consider reality a series of entities); that is, the Chinese focus on finding their own identities within a unique network of relationships with other objects and people and do not pay attention to discovering the attributes of objects or people themselves.[111] The principle of respecting contexts accords with the spirit of China's traditional culture, which means that modern personal information legislation in China needs to conform to China's situation instead of blindly copying foreign laws.

Finally, respecting contexts means respecting social reality. In daily life, everyone is a data controller, and everyone has data obligations. In other words, when individuals publish any data about their friends online or in reality, such as sharing group photos of their special moments, the publisher is processing personal data (which may expose the data of friends) and is obliged to accept inquiries from friends. Considering the information standard in the context (normal social communication), China's legislation needs to respect the actual situations of information and daily life.

In summary, only by placing inferred information within the category and analysis framework of digital human rights

can we effectively regulate and make full use of inferred information.

Declaration of Competing Interest

The authors declare no conflict of interest.

Acknowledgement

This work was supported by Research on the Theory and Practice of Legal Motivation in Contemporary China, a general project funded by National Social Science Foundation of China (Fund No. 17BFX020).

REFERENCES

Coase RH. Essays on Economics and Economists. Chicago, USA: University of Chicago Press; 1995. p. 27.

Posner Richard A. Overcoming Law, Translated by Suli. Peking, China: China University of Political Science and Law Press; 2001. p. 19.

Robotics and artificial intelligence: Ethical and legal issues. (Dec. 19,2019) https://publications.parliament.uk/pa/cm201617/cmselect/cmsctech/145/14506.htm .

Posner Richard. How Judges Think, translated by Suli. Peking, China: Peking University Press; 2010. p. 18–23.

O'Hara Kieron, Shadbolt Nigel. The Spy in the Coffee Machine: The End of Privacy as We Know It, translated by Xiaoqing Bi. Peking, China: SDX joint publishing company; 2011. p. 176–83.

Genderen Robert van den Hoven van. Privacy and data protection in the age of pervasive technologies in AI and robotics. Eur. Data Prot. Law Rev. 2017(3):347.

Murray Dan, Durrell Kevan. Inferring demographic attributes of anonymous internet users. In: Masand Brij, Spiliopoulou Myra, editors. Web Usage Analysis and User Profiling. Berlin, Germany: Springer; 2000. p. 14–18.

Cummings See ML, Roff Heather M, Cukier Kenneth, Parakilas Jacob, Bryce Hannah. Big data, algorithms, artificial intelligence and machine learning are not completely different concepts, but they are not discussed separately in this paper. Because they are inseparable from other parties in order to function, machines can store, access, and process large amounts of data; algorithms and predictions of big data are also made possible by artificial intelligence or machine learning. Machine learning is usually considered synonymous with artificial intelligence, but in fact, the former is a specific subset of the latter, and the former can be regarded as the most important and noteworthy part of the latter. Artif. Intell. Int. Aff. 2018 https://www.chathamhouse.org/sites/default/files/publications/research/2018-06-14-artificial-intelligence-international-affairs-cummings-roff-cukier-parakilas-bryce.pdf.

Ohm Paul. The many revolutions of carpenter. Harv. J. Law Technol. 2019(32):373.

General Data Protection Regulation (Dec.19,2019) https://gdpr-info.eu/.

Hildebrandt Mireille. Location data, purpose binding and contextual integrity: what's the message?. In: Floridi Luciano, editor. Protection of Information and the Right to Privacy-A New Equilibrium?. Berlin, Germany: Springer; 2014. p. 35 Louise Amoore, Data Derivatives: On the Emergence of A Security Risk Calculus for Our Times, Theory, Culture & Society. 2011(28), pp.25-30.

Derived data are produced from other data in a relatively simple and straightforward fashion, e.g., calculating customer profitability from the number of visits to a store and items bought. Inferred data are produced by using a more complex method of analytics to identify correlations between datasets and using these to categorize or profile people, e.g.,calculating credit scores or predicting future health outcomes. Inferred data are based on probabilities and can thus be said to be less "certain" than derived data. ICO, Big Data, Artificial Intelligence, Machine Learning And Data Protection, https://ico.org.uk/media/for-organizations/documents/2013559/big-data-ai-ml-and-data-protection.pdf; Rethinking Personal Data: A New Lens for Strengthening Trust, http://www3.weforum.org/docs/WEF_RethinkingPersonalData_ANewLens_Report_2014.pdf; Mireille Hildebrandt, location data, purpose binding and contextual integrity: what's the message? in Luciano Floridi (eds.), Protection of Information and the Right to Privacy-A New Equilibrium? Springer, 2014, p.39.

Jordan M. Blanke, Protection for "Inferences Drawn": a Comparison between the General Data Protection Rule and the California Consumer Privacy Act (January 12, 2020). https://ssrn.com/abstract=3518164 or doi:10.2139/ssrn.3518164.

. Profiles are regarded not as knowledge but rather as (new) data, namely, inferred data See Bart Custers, Profiling as inferred data: Amplifier effects and positive feedback loops. In: Bayamlıoğlu Emre, Baraluic Irina, Janssens Liisa, Hildebrandt Mireille, editors. Being Profiled: COGITAS ERGO SUM. 10 Years of Profiling the European Citizen. Amsterdam University Press; 2018. p. 112–15.

Like automated decisions, profiles can be based on any type of data, including derived or inferred data, such as a profile of an individual that has already been created; see Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679. "Targeting" can also be performed on inferred data; a targeter might be able to infer data about specific individuals and use that knowledge when targeting them to display ads on their social media pages; see Guidelines 08/2020 on the targeting of social media users.

Profiling works by creating derived or inferred data about individuals – "new" personal data that have not been provided directly by the subjects themselves. Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679.

Derived data refers only to data that are processed, calculated and aggregated by algorithm after the original data are recorded and stored. Therefore, data refers to the superior concept of derived data, and derived data are a specific type of data. See Lixin Yang and Xiaojiang Chen, Derived Data are the Object of Data Exclusive Rights, Social Sciences News in China, Jul.13, 2016, p.5. Shuangyang Liu and Chuan Li, Property Attributes of Derived Data and the Model of Criminal Law Protection, Academic Forum, 2020(3), pp.39-47; Shuangyang Liu, Multiple Investigations on the Approaches to Criminal Law Protection of Derivative Data, Science Technology and Law, 2020(3), pp.86-94.

Mayer-Schönberger Viktor, Cukier Kenneth. Big Data: a Revolution That Will Transform How We Live, Work and Think, translated by Yangyan Sheng. Hangzhou, China: Tao Zhou. Zhejiang People's Publishing House; 2013. p. 258.

Etzioni Amitai. Privacy in a Cyber Age: Policy and Practice. New York, USA: Palgrave Macmillan; 2015. p. 1.

O'Hara Kieron, Shadbolt Nigel. The Spy in the Coffee Machine: The End of Privacy as We Know It, translated by Xiaoqing Bi. Peking, China: SDX joint publishing company; 2011. p. 84.

Lv Shaoqing, Zhang Yuqing, Ni Ping . Privacy disclosure of social networks based on public information. J. Commun. 2013;Z1:190–6.

Mai See Jens-Erik. Big data privacy: the datafication of personal information. Inf. Soc. 2016(32):193. The distinction between data and metadata can become increasingly difficult to maintain because metadata and observation data may have the same information according to the context. The collection, linking and use of data in biomedical research and health care are ethical issues; see Nuffield Council on Bioethics https://www.nuffieldbioethics.org/wp-content/uploads/Biodata-a-guide-to-the-report-PDF.pdf.
. Similar views can be found in Chengxin Peng, How to eliminate the fundamental contradictions of data utilization-legal clarification based on privacy, information and data, exploration and free views. 2020(2), pp.79-85; Xiaying Mei, The Legal Significance of the Concept Differentiation between Information and Data. J. Comp. Law 2018;2020(6):151–62.
Rumbold John, Pierscionek Barbara. What are data? A categorization of the data sensitivity spectrum. Big Data Res. 2018(12):49–59.
Stalla-Bourdillon S, Knight A. Anonymous data v. personal data — a false debate: an EU perspective on anonymization, pseudonymization and personal data. Wisconsin Int. Law J. 2017(34):284–322.
Kuan Hon W, Christopher Millard, Ian Walden. The problem of "personal data" in cloud computing - what information is regulated? The cloud of unknowing. Int. Data Privacy Law 2011(4):225.
Hildebrandt Mireille. Location data, purpose binding and contextual integrity: what's the message?. In: Floridi Luciano, editor. Protection of Information and the Right to Privacy-A New Equilibrium?. Berlin, Germany: Springer; 2014. p. 32.
Wang Liming. New legal issues in the age of artificial intelligence. China Law Rev. 2018;2:1–4.
Xu Ming. Privacy crisis in big data era and response of tort law. China Legal Sci. 2017;1:130–49.
Pentland Alex. Social Physics: How Social Networks Can Make Us Smarter, Translated by Xiaofan Wang and Rong Wang. Hangzhou, China: Zhejiang People's Publishing House; 2015. p. 117.
Devins Caryn, Felin Teppo, Kauffman Stuart, Koppl Roger. The law and big data. Cornell J. Law Public Policy 2017(2):357–413.
. The paper presents a simple integration and supplementary explanation of the model. Louise Amoore, Volha Piotukh. Algorithmic Life: Calculative Devices in the Age of Big Data. London and New York: Routledge; 2015. p. 37–8.
Xu Ming. Privacy crisis in big data era and response of tort law. China Legal Sci. 2017(1):132.
Devins Caryn, Felin Teppo, Kauffman Stuart, Koppl Roger. The law and big data. Cornell J. Law Public Policy 2017(2):357–413.
Hildebrandt Mireille. Location data, purpose binding and contextual integrity: what's the message?. In: Floridi Luciano, editor. Protection of Information and the Right to Privacy-a New Equilibrium?. Berlin, Germany: Springer; 2014. p. 36.
Wang Liming. On the legal protection of personal information right-focusing on the boundary between personal information right and privacy right. Modern Law Sci. 2013(4):62–72.
. See the definition of "personal information" in Article 1034 of the Civil Code of the PRC: "personal information is a variety of information recorded electronically or in other ways that can identify a specific natural person alone or in combination with other information, including the name, date of birth, ID number, biometric information, address, telephone number, e-mail, health information, whereabouts information, etc.", and the provisions of California Consumer Privacy Act (CCPA)(1798.140(o)): "Personal information means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." In GDPR Article 4(1), personal information is any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. "Relating to" and "about" define the connective process that links an individual to a recognizable and applicable process of identity. Legal practice in Australia states that if an individual's identity is apparent or reasonably ascertainable, or under the current definition is identifiable or reasonably identifiable, then data should be deemed to be about an individual and be classed as personal information. "About" obtains its statutory application from the notion of identity. See Mark Burdon, Digital Data Collection and Information Privacy Law. Cambridge University Press; 2020. p. 159–68.
. Self-determination of personal information encourages the use of data, and this kind of right to self-determination of personal information may also include property rights. See Xuxu He, The Right to Self-Determination of Personal Data in Comparative Law. J. Comp. Law 2013(2):72–3.
Jordan M. Blanke, Protection for "Inferences Drawn": A Comparison between the General Data Protection Rule and the California Consumer Privacy Act (January 12, 2020). Available at SSRN: https://ssrn.com/abstract=3518164 or http://dx.doi.org/10.2139/ssrn.3518164. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3518164. Wachter, Sandra and Mittelstadt, Brent, A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI (October 5, 2018). Columbia Business Law Review, 2019(2), Available at SSRN: https://ssrn.com/abstract=3248829. The 2012 Personal Data Protection Act in Singapore also does not consider the authenticity of data; the inferred information can be regarded as personal information. Personal Data Protection Ac t 2012, https://sso.agc.gov.sg/Act/PDPA2012.
Liu Yahui, Zhang Tieying, Jin Xiaolong, Cheng Xueqi. Privacy protection in big data era. J. Comput. Res. Dev. 2015(1):229–47.
Solove Daniel J. I've got nothing to hide and other misunderstandings of privacy. San Diego Law Rev. 2007:745–72 vol.44.
Hu Ling. Internet privacy protection: a perspective of information production and architecture. Law Soc. Sci. 2009(2):64–90.
Wachter Sandra, Mittelstadt Brent. A right to reasonable inferences: re-thinking data protection law in the age of big data and AI (October 5, 2018). Columbia Bus. Law Rev. 2019(2):12–14. Available at SSRN https://ssrn.com/abstract=3248829.
Zhang Yujie. A legal review of the automatic completion function of search engines. Law Sci. Mag. 2019(5):122–31.
Wang Rui, Xiong Jian, Huang Guiqin. Legal thoughts on perfecting China's personal credit information system. China Legal Sci. 2002(4):82–94.
Xiong Jingwen. Constitutional control of search in the age of smartphones. Hum. Rights Res. 2019. Dec.20 http://law.suda.edu.cn/32/a2/c996a12962/page.htm.
Xiong Jingwen . Constitutional control of search in the age of smartphones. Hum. Rights Res. 2019. Dec.20 http://law.suda.edu.cn/32/a2/c996a12962/page.htm.
Tesla customer privacy policy. (Dec.5,2019)https://www.tesla.cn/about/legal.
O'Neil Cathy. Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy, translated by Ruisong Xu. Taipei, Taiwan: Briefing Press; 2017. p. 88–92.
Solove Daniel J. Understanding Privacy. Cambridge, Massachusetts, USA: Harvard University Press; 2010. p. 1–7.
Privacy and Information Technology, Stanford Encyclopedia of Philosophy. (Dec.12,2019)https://plato.stanford.edu/entries/it-privacy/.

Kift Paula, Nissenbaum Helen. Metadata in context-an ontological and normative analysis of the NSA's bulk telephony metadata collection program. J. Law Policy Inf. Soc.; 2017. p. 334–5.
Rubel Alan. Legal archetypes and metadata collection. Wisconsin Int. Law J. 2017(4):823–53.
Ren Danli. The right structure of personal information viewed from the debate between Shunfeng Co. and Cainiao Co.. Polit. Sci. Law 2018(6):135.
Search King, Inc. v. Google Technology, Inc., Case No. CIV-02-1457-M (W.D. Okla. May. 27, 2003).
Langdon v. Google, Inc., 2007 WL 530156, Civ. Act. No. 06-319-JJF (D. Del. February 20, 2007).
Jian Zhang v. Baidu.Com Inc., 10 F. Supp. 3d 433 (S.D.N.Y. 2014).
Zuo Yilu. Algorithms and speech: theory and practice in US. Glob. Law Rev. 2018(5):122–39.
Liu Jinrui. Personal Information and Allocation of Rights: Reflections on the Right of Self-determination of Personal Information. Peking, China: Law Press•China; 2017. p. 123.
Hildebrandt Mireille. Location Data, Purpose Binding and Contextual Integrity: What's the Message?. In: Floridi Luciano, editor. Protection of Information and the Right to Privacy-A New Equilibrium?. Berlin, Germany: Springer; 2014. p. 38.
Nissenbaum Helen. Privacy in Context: Technology, Policy, and the Integrity of Social Life. California: Stanford University Press; 2009. p. 42–9 p.56.
Productivity Commission Inquiry Report (2017), Data Availability and Use, (Jul.2,2019) https://www.pc.gov.au/inquiries/completed/data-access/report/data-access.pdf.
Harris Peter. Data, the European Union General Data Protection Regulation (GDPR) and Australia's New Consumer Right; 2019 (Jul.9 https://www.pc.gov.au/news-media/speeches/data-protection .
Schwartz Paul M, Peifer Karl-Nikolaus. Transatlantic data privacy. 106 Georgetown Law J. 2017;115:115–79.
Consumer Online Privacy Rights Act, https://www.cantwell.senate.gov/imo/media/doc/COPRA%20Bill%20Text.pdf.
"Infer" or "inference" means the derivation of information, data, assumptions, or conclusions from facts, evidence, or another source of information or data, and personal information includes inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes (1798.135).
Grafanaki Sofia. Autonomy challenges in the age of big data, Fordham Intellectual Property. Media Entertain. Law J. 2017(4):803–68. FTC Staff Report (2015), Internet of Things: Privacy & Security in a Connected World https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-November-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.
Simson L. Garfinkel. De-Identification of Personal Information, (Aug.6,2019) http://dx.doi.org/10.6028/NIST.IR.8053.
Jin Yao. Legal basis and norm reconstruction of personal information de-identity. Law Rev. 2017(3):120–9.
GDPR Focuses on Personal Data (collected) Rather Than Inferred Data Such as Knowledge. In the Context of the EU, Legal Terms Such as "Processing" and "Use" can Actually Include "Infer"; that is, Inferred Data are Widely Used for Data Processing and Profiles.
General Data Protection Regulation (GDPR), Article C, (Jul. 21, 2019) https://gdpr-info.eu/.
Liu Jinrui. Personal Information and Allocation of Rights: Reflections on the Right of Self-determination of Personal Information. Law Press•China; 2017. p. 112.
Ibid, p.123.
Australian Law Reform Commission. For your information: australian privacy law and practice (ALRC Report 108), (Sept.5,2019) https://www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/.
Zhang Yujie. A legal review of the automatic completion function of search engines. Law Sci. Mag. 2019(5):122–31.
. Criminal Law of the People's Republic of China; 2020 (Jan.16 https://www.66law.cn/tiaoli/9.aspx .
. Civil Code of the People's Republic of China; 2021 (Feb.6 https://www.66law.cn/tiaoli/153012.aspx .
. Cyber Security Law of the People's Republic of China; 2020 (Jan.16 https://www.66law.cn/tiaoli/9874.aspx .
. Decision of the Standing Committee of the National People's Congress on Strengthening the Protection of Network Information; 2020 (Jan.16 https://www.66law.cn/laws/84143.aspx .
. Provisions on the Protection of Personal Information of Telecommunications and Internet Users; 2020 (Jan.16 https://www.66law.cn/tiaoli/6435.aspx .
Hu Wentao. Conceptions on the definition of personal sensitive information in China. China Law Sci. 2018(5):235–54.
(2019) Zhe 8601 Xing Bao No.1Civil Ruling.
Zhou Jiahai, Zou Tao, Yu Haisong. Interpretation and application of several issues on the application of laws in handling criminal cases involving citizens' personal information. People's Judicature 2017(19):31–7.
Who Moved My Address Book? The terrible situation of App over-collecting user information. (Aug.8,2019) https://mp.weixin.qq.com/s/S3yBwwqeFmmxctxtjY7ruQ.
(2013) Shen Bao Fa Zhi Min Chu Zi No.28.
(2017) Yue 03 Min Zai No.138.
Gao Fuping. Personal information protection: from personal control to social control. Chin. J. Law 2018(3):84–101.
Schwartz Paul M, Peifer Karl-Nikolaus. Transatlantic data privacy. 106 Georgetown Law J. 2017;115:115–79.
See Kift Paula, Nissenbaum Helen. Metadata in context - an ontological and normative analysis of the NSA's bulk telephony metadata collection program. J. Law Policy Inf. Soc. 2017(13):334.
See Nissenbaum Helen. Privacy in Context: Technology, Policy, and the Integrity of Social Life Stanford University Press; 2010. p. 132.
Nissenbaum Helen. Contextual Integrity Up and Down the Data Food Chain. Theoretical Inquiries in Law 2019;2019(20):227.
See Lessig Lawrence. Code: Version 2.0, translated by Xu Li & Weiwei Shen Tsinghua University Press; 2009. p. 93–4.
Similarly Robert. Post believes that the core of all "branches" in privacy is the sanctity of community norms. Communities have established their own self-concept through socialization. When these norms are threatened (for example, by the invasion of private socialization), the individual's personal identity is in jeopardy. Therefore, the right to privacy is protected by determining and protecting norms and requiring respect for others' norms. Will Thomas DeVries, Protecting Privacy in the Digital Age. Berkeley Technol. Law J. 2003(18):310.
Nissenbaum See Helen. Privacy as contextual integrity. Washington Law Rev. 2004(79):155.
Some scholars believe that "contextual integrity" refers to the purpose and common interests of a certain social group. In the era of big data, whether privacy interests exist should be determined based on the relationship between the right holder and that person's counterpart in a specific social group. Different social groups have different organizational purposes, so relationships among members also differ. For details, please refer to Weiguang Wu, Understanding the

Particularity of China's Privacy System from the Generation and Essence of Privacy Interests, in Contemporary Law Review, 2017(4), p. 54.
Nissenbaum See Helen. Respecting context to protect privacy: why meaning matters. Sci. Eng. Ethics 2018(24):831–52.
Martin Kirsten E, Nissenbaum Helen. What is it about location? Berkeley Technol. Law J. 2020(1):254–6.
The Civil Code lists "privacy and personal information protection" as a separate chapter of personality rights, but the law stipulates only that "personal information of natural persons is protected by law" and does not identify it as a right. There may be two considerations for the legislature: (1) whether personal information can be proven to be a right is theoretically doubtful, and (2) China has reservations about the protection of personal information and places more emphasis on data circulation.
The draft strongly emphasizes the regulation of inferred information. For example, Article 25 states that the use of personal information for automated decision-making should ensure the transparency of processing and the fairness and reasonableness of the results. If an individual believes that automated decision-making has a significant impact on his or her rights and interests, he or she has the right to ask the processor to explain and to refuse the decision made only through automation. For commercial marketing and information pushed through automatic decision-making, options that are not specific to the individual's personal characteristics should be provided at the same time. There are many references to international mainstream personal information protection laws (such as the GDPR) and technical specifications, such as the informed consent principle and purpose restriction principle (Article 13 to Article 24), risk assessment strategies (Article 54) and many personal information rights (Article 44 to Article 49). https://www.sohu.com/a/426342159_120626422.
The Anti-monopoly Guide of the Anti-monopoly Committee of the State Council on the Platform Economy (Guo Fan Long Fa [2021]No.1), Article 17 prohibits operators in the platform economy from using big data and algorithms (according to the payment ability, consumption preference and usage habits of the counterparty), abusing the dominant position of the market, and implementing differential treatment for counterparties with the same trading conditions without justifiable reasons. Article 15 of The Interim Provisions on the Administration of Online Tourism Business Services issued by the Ministry of Culture and Tourism on October 1, 2020, also stipulates that online tourism operators shall not abuse technical means such as big data analysis to infringe the rights and interests of tourists based on tourists' consumption records and travel preferences.
On November 26, 2020, the Ministry of Industry and Information Technology and the Telecommunications Terminal Industry Association jointly issued the "Minimum Necessary Evaluation Specification for app Collection and Use of Personal Information", which emphasizes the limitations of context and purposes: the type, quantity and frequency of collecting personal information should follow the principle of minimum necessity; that is, the type of personal information collected and used should not exceed the actual needs of business contexts, and APP should establish an independent control mechanism for personal information (such as labels and portrait dimensions) for users, ensuring that users can control the relevance of a directional push display. The Interim Provisions on the Protection and Management of Personal Information of Mobile Internet Applications, which are being drafted, clearly define two basic principles of personal information protection: informed consent and minimum necessity. The principle of informed consent requires that users be informed of the rules of personal information processing in clear and understandable language, and users should make voluntary and clear indications with full support.
(2017) Jing 01Min Zhong No.509 civil judgement.
(2020) Yue 0305 Min Chu No.825 civil judgement.
Rethinking Personal Data: Trust and Context in User-Centred Data, (Nov.6, 2019) http://www3.weforum.org/docs/WEF_RethinkingPersonalData_TrustandContext_Report_2014.pdf.
Helen Nissenbaum. A Contextual Approach to Privacy Online (2011). Daedalus 140 (4), Fall 2011: 38. Available at SSRN: https://ssrn.com/abstract=2567042.
Nissenbaum Helen. Contextual integrity up and down the data food chain. Theor. Inq. Law 2019;Vol.20(1):221–56.
O'Neil Cathy. Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy, translated by Ruisong Xu. Taipei: Briefing Press; 2017. p. 222–6.
Nissenbaum Helen. Privacy in Context: Technology, Policy, and the Integrity of Social Life. California: Stanford University Press; 2009. p. 179–80.
Rethinking Personal Data: Trust and Context in User-Centred Data,(Nov.6, 2019) http://www3.weforum.org/docs/WEF_RethinkingPersonalData_TrustandContext_Report_2014.pdf.
Ibid.
Needham Joseph, Ronan Colin A. Cambridge, UK: Cambridge University Press; 1978. p. 78.