Scientific Research Publishing

Beijing Law Review, 2022, 13, 626-639
https://www.scirp.org/journal/blr
ISSN Online: 2159-4635
ISSN Print: 2159-4627

Legal Attributes of IP Attribution Information under China's PIPL: Clarification of Identifiability Terminology and Operationalisation of Identifiability Criteria

Chaolin Zhang[1*], **Geng Wang**[2]

[1]Law School, Nankai University, Tianjin, China
[2]Law School, University of International Business and Economics, Beijing, China
Email: *zhang_chaolin@163.com

How to cite this paper: Zhang, C. L., & Wang, G. (2022). Legal Attributes of IP Attribution Information under China's PIPL: Clarification of Identifiability Terminology and Operationalisation of Identifiability Criteria. *Beijing Law Review, 13,* 626-639.
https://doi.org/10.4236/blr.2022.133040

Received: August 20, 2022
Accepted: September 20, 2022
Published: September 23, 2022

Abstract

Major Chinese internet platforms recently introduced the function of revealing users' IP attribution information. However, it is unclear whether such information fall under China's PIPL's definition of "personal (identified) information", as the law does not clearly define the identifiability terminology, nor does it provide an operational approach to the identifiability criteria. Combining research methods such as comparative law studies and case studies, this difficulty in the application of the PIPL can be resolved from two mutually complementary directions. First, the identifiability terminology in China's PIPL can be specified into three different sets of connotations, only one of which needs to be satisfied by the target information: direct or indirect identification, identified or possible identification, identity or feature identification. Secondly, the identifiability criteria can be made operational through a joint horizontal and vertical evaluation system in which the following two elements must be satisfied simultaneously: the horizontal distinction between the target user and other users, and the vertical counterpart between the target message and the target user. In particular, it is more appropriate for the practitioners of China's PIPL to tackle their vertical counterpart evaluation with the "subjective/relative approach". By using the aforementioned methods, it may be proven that IP attribution information qualifies as "personal information" under Chinese law and society. Other information with unclear legal attributes can also benefit from the above general approach and deductive demonstration.

Keywords

IP Attribution Information, China's Personal Information Protection Law, Personal Information, Identifiability, Network Real-Name System

1. Introduction

Recently, several large Chinese Internet platforms, including Sina Weibo, Douyin, Today's Headlines, WeChat (Official Account), Xiaohongshu, and others, have made users' Internet Protocol attribution information (hereinafter "IP attribution information") public. The specific changes brought about by this measure are that domestic accounts display the province (autonomous region, or municipality) information where the user is located while foreign accounts display the country or region information and that users are not allowed to turn this function off on their own.

According to the official announcements of these major platforms, the purpose of their online reveal of the IP attribution information can be summarized as combating the three types of undesirable practices listed below. Firstly, there are a large number of users posing as people from specific regions and creating and fabricating internet-based rumours, which leads to a breakdown in the order of communication in the context of major events and prevents real and valid information from being accessed promptly. The trigger for Weibo to disclose users' IP affiliation was that during the Russian-Ukrainian conflict, many users on the platform posed as people in Ukraine and posted false information; during the outbreak of the COVID-19 epidemic in Shanghai, some accounts published a large number of posts sadfishing, asking for help and breaking news, but after this function was launched, these users were found by other netizens that many of them were not in Shanghai, and the messages they posted was also confirmed to be false after investigation (He, 2022). Secondly, online violence magnifies moral anomie in the process of societal modernisation, and the "depicted" online events violate the group's ethical values. The group's value judgment thinking only distances public opinion from the facts themselves (Wang, 2022: p. 29, 31), and the network platform becomes a place for the group to blindly vent their emotions. For the person in question, the violence of these statements in virtual space can be mapped to their real life, interfering with their normal social relationships and interactions and increasing the likelihood of depression, suicide, and other extreme cases (Ren & Wang, 2020: pp. 155-157). Thirdly, with the development of cyber bots technology, the manipulation of public opinion has been increasingly automated, efficient and adaptive (Li et al., 2020: p. 35), which has made it significantly more difficult for platforms to respond. Usually, as long as specific keywords are preset in the system when these keywords are mentioned in the user's speech, the bot will be triggered and automatically disguised as a real user to leave a message. This is often the case with fans who are trying to make their idols look good, and with anti-Chinese forces who incite and guide them, as in the case of the "5 g Chinese toothpaste experiment"[1],

[1] User only needs to post online in Chinese: "I only use Chinese toothpaste for clean brushing and only use 5 g each time [我牙膏只用中华为的是刷的干净，而且每次只用 5 g 就行了]". Due to Chinese language conventions, this post contains the words "Huawei [华为]" and "5G". As the system has set these two words as the trigger for automatic comments by bots, these bots have automatically followed up with comments attacking Huawei and 5G.

which has been widely circulated in the Chinese internet platforms (Aoligei Say, 2022).

To a certain extent, the data processing behaviour of these platforms in revealing information on the IP attribution of their users is legitimate. The aforementioned pressure on the platform is partially alleviated by the act of publicly revealing the IP attribution information of all users, although this may be of limited use. Most directly, this function provides users with a basis for identifying information on the Internet, and IP affiliation information can at least be used as a reference to corroborate the authenticity of the content. Next, this function will alert and warn against arbitrary speech, helping to curb illegal speech such as disinformation, defamation, superstition, hatred and division, thus reducing the negative and even extreme social atmosphere in the Internet public space. Besides, this function can directly reduce the phenomenon of impersonating parties from a specific geographical area for newsjacking, so that other users can clearly distinguish between them. More crucially, this function will help to combat cyber bots and thus reduce fan domination of comments and manipulation of public opinion by anti-Chinese forces, as the overly consistent information on IP attribution will provide a clear guide to quickly identify targets for censorship.

However, since the reveal of the IP attribution information applies to all users within these platforms without distinction and no user can refuse this reveal, it is perfectly natural that this has led to extensive public debate about this data processing practice. The general question is whether the launch of this feature will violate users' rights to personal information. Specifically, the user's IP attribution information is forcibly disclosed by the platform during the process of posting and leaving messages, and the content of the information being processed matches the user's real situation; furthermore, the user has no room for self-determination regarding this data processing behaviour.

From the perspective of existing laws and regulations, the current rules do not provide clear guidance to resolve the controversy. The key is that the Personal Information Protection Law of the People's Republic of China (hereinafter "China's PIPL" or "the PIPL") which is the basic law in the field of information protection does not explicitly state whether the IP attribution information falls within the scope of personal information in the context of the law, resulting in an unclear expectation of the legal application of whether the rights and interests of individuals are protected. The root of this problem is that the PIPL uses identifiability attributes as the basis for determining whether the disputed information is personal information for the law, but the legislator has been vague about how to understand the identifiability terminology and how to apply the identifiability criteria.

This article will examine each of these concerns and offer specific solutions. The second part clarifies the uncertainties that exist in the terminology identifiability under the PIPL and attempts to define its connotations. The third part further analyses the identifiability criterion under the PIPL and provides an easily operationalised and readily accepted assessment method through traditional legal research methods such as case studies and comparative law studies. At the same time, this part will also incorporate an analysis of the gains and losses of cutting-edge extraterritorial experience. Together, these two sections provide a universal approach to understanding and applying the term "personal information" in the PIPL. The fourth section will show how these provided methods have been interpreted and applied to real-life cases and substantially answer the central concern of this paper, i.e., whether users' IP attribution information is the "personal information" under China's PIPL.

2. Indeterminacy in Identifiability Terminology in the PIPL and Its Clarification

Personal information is a threshold concept for the application of data protection law generally: if data being processed are not personal data, their processing is not subject to such law (Bygrave & Tosoni, 2020: p. 105). Article 4 of the PIPL expressly defines "personal information" as "all kinds of information, excluding anonymized information, recorded electronically or otherwise, relating to an identified or identifiable natural person". As is common practice in other countries with data protection laws (Bygrave & Tosoni, 2020: p. 108), China's PIPL orients the identifiability terminology at the core of the concept of "personal information". The phrase "personal information" is used to denote information from individuals, and "identified information" is used to denote information that identifies individuals. Therefore, identifying information is personal information, but personal information is not necessarily identified information (Garfinkel, 2015: p. 3). From this perspective, China's PIPL limits the scope of personal information it aims to protect to personal identified information.

However, the legislator does not further define the key terminology "identifiability" and leaves room for interpretation (Cao, 2022: p. 133), which is necessary and desirable. To be precise, the term "identifiability" is both a standard set by the law and an objective factual state and not all information processing that can in fact be identified is covered by the PIPL. At the same time, from the perspective of data science, the identifiability of personal information is not as stable as the object, but changes with the subject who owns the data, the scenario of use, the duration of data retention, and the development of technology, which determines the scenario and dynamic nature of the definition of personal information (Qi & Zhang, 2018: p. 126). Therefore, the gap between the factual and legal nature of the identifiability terminology is where the interpretation space reserved by the Law lies, and the existence of this interpretation space provides tension and flexibility so that the practitioners of the law can flexibly adjust the aforementioned jurisdictional scope on a case-by-case basis.

Increased flexibility is usually accompanied by a decrease in certainty, and the scope for interpretation of identifiability creates difficulties in the practical application of the PIPL so legal certainty must be enhanced by legal interpretation. In practice, it is common for legal provisions or language to be ambiguous and require interpretation; however, the controversy arises not because the legal language itself is ambiguous, but because there is a disagreement about the scope of application that the law should cover (Su, 1997: p. 18). Through a review of current legal norms and judicial practice, this article finds that the personal information intended to be governed by Chinese personal information protection laws can be broadly divided into three levels, each pointing to a different dimension of identifiability:

1) The regulation of the PIPL points to direct identification and also covers indirect identification. For example, in the case of Yu v Beijing Kuche Yimei Network Technology Co., Ltd. (Vehicle Identification Number Case, hereinafter called the VIN case)[2], the central point of contention between the parties lies in whether the VIN on the vehicle registration certificate is personal information. The judge, in that case, held that as neither direct nor indirect identification was required, the frame number was not personal information for Article 1034 of the Civil Code of the People's Republic of China (2020) (hereinafter "the Civil Code")[3].

2) Article 4 of the PIPL further refines the term identifiability in the Civil Code to "identified or identifiable", which is intended to indicate that the law not only protects the rights and interests of personal information that have already been damaged but also has the intention to protect the rights and interests of personal information that may be at risk of being damaged.

3) Identifiability encompasses both identifications of individual identity and identification of individual characteristics; identification of individual identity determines who the information subject is, while identification of individual characteristics determines the type of person the information subject is. This proposition was clearly articulated by the judges of the Beijing Internet Court in their decision in the case of Ling v Beijing Weibao Vision Technology Co., Ltd.[4].

For disputed information, these three dimensions are not mutually exclusive, nor are they required to be satisfied at the same time; they are intertwined and mixed. Disputed information may be "identified" in different dimensions at the same time.

3. Operationalisation of the Identifiability Criterion in the PIPL: Joint Horizontal and Vertical Assessment

The three levels described above frame the scope of personal information governed by PIPL in terms of content, and it is then necessary to address how the identification criteria can be practically understood and applied on this basis. An effective way to do this is to interpret the identification criteria themselves, and this paper argues that the horizontal distinction between specific users and other users, and the vertical counterpart between information and specific users, constitute a joint horizontal and vertical evaluation system for the identifiability cri-

[2] Yu v Beijing Kuche Yimei Network Technology Co., Ltd. (2021) Yue 0192 Min Chu No. 928.

[3] At the time the VIN case was brought to court, China's PIPL was not yet in force. Therefore, the parties invoked the relevant provisions of the Civil Code rather than the PIPL and the court's decision was based on the Civil Code.

[4] Ling v Beijing Weibao Vision Technology Co Ltd. (2019) Jing 0491 Min Chu No. 6694.

teria.

3.1. Horizontal Distinction Assessment and Its Convergent Evolution

The horizontal distinction aspect is used to assess whether the information at issue distinguishes the subject of the information from other individuals. In general terms, a natural person can be considered as "identified" when, within a group of persons, he or she is "distinguished" from all other members of the group (Art. 29 WP, 2007: p. 12). This element of the assessment may not require much explanation in terms of understanding and use, as it is very clear and unambiguous and its desired outcome is easy to judge intuitively. The only thing that might need to be mentioned is the status, relationship and order of application between this element of the assessment and the other element, the vertical counterpart. Taken as a whole, both elements need to be satisfied to meet the criteria for recognition established by China's PIPL. From a more detailed point of view, it may be more convenient to give priority to the assessment of the vertical counterpart. More precisely, when the link between the target information and a particular individual is confirmed, this has cut off that information from other subjects from one side; in other words, the horizontal distinction is completed at the same time as the process of judging the vertical counterpart.

In addition, the horizontal distinction assessment may be a good platform to demonstrate some developments on the third level of identifiability terminology, identity or feature identification. Leenes (2007: pp. 141-142) proposed a fourfold classification of identification and distinguished look-up, recognition, classification, and session identifiability. According to Leenes, identity identification is more than just establishing citizenship, and we must read extensively about identity if we are to truly address privacy and personal information protection concerns. With the widespread adoption of big data technology, the role of identity identification becomes more limited, while feature recognition takes on a larger role. The latest study by Purtova (2022) keenly captures this change and adds targeting as the new fifth identification type, implying the selection of a specific individual from a group at a point in time as the object of attention or processing. It is not difficult to find convergence between the above theory's evolution and Chinese judicial practice. This justifies the horizontal distinction as a constituent element of the personal information identification criterion: this element is both geographically universal, which justifies it in a general sense, and at the same time it has proved to be somewhat resilient to accommodate the development of real-life situations.

3.2. Vertical Counterpart Assessment and Its Differences in Judicial Practice in Different Countries

The second aspect is the vertical counterpart, which is used to assess the extent of the relationship between information and the subject, as well as whether the

PIPL setting is met. China's PIPL adds the word "relevant" to the definition of personal information compared to the Civil Code, and some scholars have pointed out that this is a reference to the General Data Protection Regulation (hereinafter "GDPR"), which adds the criterion of association to the criterion of identification (Wang & Ding, 2021: p. 2). In other words, there are two paths to determine whether an item of information is personal information: one is identification, from the information to the individual; the other is an association, from the individual to the information (Wu, 2022: p. 417). A more general understanding of these two criteria is that both identification and association are essentially about the "vertical counterpart" between the information and the individual.

The courts usually have a certain degree of discretion in relation to this vertical counterpart assessment. The existing experience of judicial practice shows that there are significant differences in the approach of the Chinese courts and the EU courts, which make a comparative analysis necessary and valuable. In brief, the former sets a relatively high threshold for assessing vertical correspondence, and only close, necessary connections are the identifying relationships that China's PIPL is designed to regulate; however, the EU courts have a very broad understanding and are in line with the trend of case law, more and broader identifying relationships will fall under the jurisdiction of the GDPR.

To determine whether the information in question is individually identifiable, Chinese courts require a relatively close degree of correspondence. In the aforementioned VIN case, for example, the judge held that the condition information about the vehicle could only identify a specific vehicle and that the interference of many realities could sever the inevitable link between that vehicle and its owner, for example, the use of the vehicle by family members and garage employees could reduce the direct correlation between the owner and the condition information. In addition, to analyse the possibility of indirect identification of vehicle condition information, the Court considered objective factors such as the cost, time and technology required for a third party to identify a natural person by their VIN and concluded that the likelihood of identifying personal information under such realistic conditions was low. As to how to take into account the objective factors, Zhao (2021: p. 135) provides specific methods: firstly, the material basis required for the identification of a specific natural person should be considered and the cost of this identification should not exceed the legal interest to be protected for identification; secondly, the technical requirements and economic costs of achieving the legal identification should be considered. The distillation of this approach is based on an analysis of the evolution of relevant legislation, judicial practice and mainstream theory in China, and is therefore naturally applicable and reasonable for understanding the identifiability criteria for PIPL.

However, the European Court of Justice (hereinafter "CJEU") has evolved from a relatively restrictive understanding of "counterpart" to a very broad one, whereby information that would be considered insufficiently relevant in China's courts would be regarded as personally identifiable information from the CJEU's perspective. In the earlier case, YS and others, the CJEU interpreted "relating to" in a very restrained manner[5]. The Court held that "the legal analysis of a particular immigration eligibility application made by the relevant authority, although it may contain personal data, the legal analysis itself is not such data within the meaning of the 95 Directive and is not relevant to the protection of the person's right to privacy"[6]. Two years later, in the Patrick Breyer case, the Court's perspective shows an expansive change[7]. In particular, the CJEU began to favour a more "subjective/relative approach" that focuses on the online media service provider's possibility of (potentially) identifying an individual and whether it has the legal and practical means which enable it to do so with additional data a third party has about that person (this means third party knowledge needs to be considered but only to a certain extent) (Niemann & Schuessler, 2016). It can be observed that the logic, approach and outcome of the CJEU, in this case, is similar to the approach of the Chinese courts in the VIN case. Coincidentally, the information at issue, in that case, was IP address information, which is related to and must be distinguished from the IP attribution information discussed in this article. The necessary analysis will be presented further in Part 4.

As opposed to the "subjective/relative approach", the "absolute/objective approach" adopted by the domestic law of some EU Member States, according to which data is already considered "personal data" if any third party worldwide can identify the individual (Niemann & Schuessler, 2016). This absolute/objective approach was formally introduced in the Peter Nowak case[8] in 2017. The CJEU did not uphold the High Court's reference to YS and others *case*. According to the CJEU, whether the examiner was able to identify the candidate when correcting and marking the examination paper was irrelevant, as long as the information was "relating to" the data subject, whether objective or subjective, it could constitute personal information under the provision[9]. Under the implications of the case, the vertical counterpart criterion of the CJEU will be satisfied as long as one of the three—content, purpose or effect of the information—is linked to a specific person. To a certain extent, the vertical counterpart at this point has moved away from identifying criteria and has become incredibly inclusive, even without borders. As one widely cited viewpoint points out, when the hyper-connected online world of data-driven organisations arrives, the GDPR's intensive compliance regime will become "the law of everything", well-intentioned but unassailable (Purtova, 2018: p. 40).

[5] YS (C-141/12) v Minister voor Immigratie, Integratie en Asiel, and Minister voor Immigratie, Integratie en Asiel (C-372/12) v M,S. in Joined Cases C-141/12 and C-372/12, ECLI:EU:C:2014: 2081, Judgment of 17 July 2014.

[6] Ibid, para. 39, 45.

[7] Patrick Breyer v Bundesrepublik Deutschland, Case C-582/14, ECLI:EU:C:2016:779, Judgment of 19 October 2016.

[8] Peter Nowak v Data Protection Commissioner, Case C-434/16, ECLI:EU:C:2017:994, Judgment of 20 December 2017. The Irish Supreme Court referred the following question to the CJEU for a preliminary ruling: Can information recorded on answers given by candidates during professional examinations be considered personal data under Directive 95/46?

[9] Ibid, para. 30-34.

Even if, to resolve the same dispute, judicial experience from the application of EU law does not necessarily apply in China, the crisis triggered by the former's relatively radical trend can sound a warning bell for the proper application of Chinese law. It could be argued that this lack of restraint in the EU's understanding creates a data governance conundrum: overly broad presuppositions of rights protection can raise the cost of maintenance too high, leading to protections that are effectively hollowed out. As consumers have privacy expectations when using the Internet, it may be difficult to agree that all expectations are worth meeting, so a privacy theory is required to make the distinction, examining which privacy expectations must be met and which do not (Nissenbaum, 2018: p. 841). Similarly, China's PIPL has a specific context and a specific scope of protection: the PIPL covers the handling of personal information that has a significant impact on the subject's rights and interests, whereas the use of personal information, in general, is left to other laws, industry norms, or social customs (Gao, 2021: p. 81). It is therefore more appropriate for China's PIPL practitioners to adopt the subjective/relative approach to the judgement of vertical counterparts.

4. Deduction and Application: Whether IP Attribution Information Is Personal Information Covered by China's PIPL?

What follows is a substantive investigation into the central question of whether IP attribution information should be considered personal (identifiable) information in the context of China's PIPL. During this process, the aforementioned criteria will be shown how they are applied in practice.

4.1. The Distinction between IP Attribution Information and Adjacent Concepts

Before dealing specifically with the legal attributes of IP attribution information, a *de facto* distinction needs to be made between this concept and two other information concepts: IP addresses information and the physical location information of users. IP addresses are a uniform address format provided by the IP protocol. Every user visit on the Internet is from one IP address to another, and the principle of the protocol dictates that the two parties communicating must know each other's IP addresses, but IP addresses themselves do not have a physical location function (Liu & Lu, 2002: p. 83; Cheng, 2008: p. 26; Wen & Xiao, 2022: p. 62). IP addresses, as a limited number of resources, are allocated to institutions and organisations in a fixed register, while IP attribution information depends on which organisation the IP address is allocated to. As a basis for other work in website management, the Chinese authorities require all websites to register their domain and IP addresses and have established a database of the domain and IP addresses (Yu & Ye, 2018: p. 422). The IP address database will infer the approximate city of the IP address based on the initial registration, which is the province information or country or region information currently displayed on the Chinese platforms.

In practice, IP attribution information may not match both the IP address and the physical address of the actual visitor, in two common cases: firstly, where the organisation with the IP address is used across the province[10], and secondly, where there is interference from the base station signal switching[11]. In fact, the generation of IP address and IP attribution information does not require the user to authorise and open the physical location rights of the device used, nor is it necessarily linked to the user's actual location information.

Therefore, the conclusion that can be drawn from a data science perspective is that the three concepts have their specific meanings and are not to be used interchangeably in a general way; however, it is undeniable that the three are so closely linked that they can be exactly equivalent under certain conditions. Thus, the actual relationship between the three needs to be analysed on a case-by-case basis in specific scenarios.

4.2. IP Attribution Information Fall under the Concept of "Personal Information" in China's PIPL

It is necessary to briefly recapitulate the findings in Parts 2 and 3 here. First, the connotation of the term identifiability under China's PIPL has three dimensions, and the law is satisfied in terms of content when the reality of the situation satisfies any one of them. Secondly, the criterion set by the law for identifiability can be understood as two elements of evaluation, horizontal distinction and vertical counterpart, and the target information needs to satisfy both elements.

What needs to be determined is whose/which group's identifiability should be the object of analysis to evaluate the identifiability of IP attribution information in general. Currently, judicial practitioners in China's PIPL prefer a subjective/relative approach to the vertical counterpart of the identifiability criterion. This approach focuses on the online media service provider's possibility of (potentially) identifying an individual and whether it has the legal and practical means which enable it to do so with additional data a third party has about that person (Niemann & Schuessler, 2016). Therefore, it needs to be further clarified what additional data these online media service providers hold about their subscribers, in addition to their IP attribution information.

Within the legal context of China's Internet platform regulation, the online real-name system is a fundamental institution, and this system is under the principle of "mandatory registration of the legal name in the background and voluntary use of the legal name as screen name"[12]. To comply with the provi-

[10] If a company has a nationwide intranet, but employees use the IP of the head office when accessing the extranet, then eventually the IP attribution information presented to everyone in the company will be the head office's IP attribution information.

[11] The mobile phone's base station has a certain coverage area, and usually there are two or three different base stations in different directions at the same time where a mobile phone is located. If the signal strength of the two base stations is similar, the actual base station connected to the phone at the border of the two provinces may be constantly switching, and the IP attribution information displayed when posting may change between the two provinces.

[12] According to the Article 24 of the Cybersecurity Law of the People's Republic of China (2017), Article 5 of the Provisions on the Administration of Account Names of Internet Users (2015), and Article 5 of the Provisions on the Administration of Internet Comments Posting Services (2017), Internet platform users are required to provide their real identity information when registering an account in the background and are free to choose whether to express themselves through anonymity when speaking publicly in the foreground.

sions of this system, Internet platforms require users to authenticate their real identity information upon registration. This rule is mandatory (Xie, 2015: p. 48) and these platforms are not allowed to provide relevant services, such as information distribution and instant messaging, to users who do not provide their real identity information. On 1 August 2022, the Provisions on the Administration of Internet Users' Account Information come into force. Article 9 of the regulation further clarifies that the real identity information used for authentication includes the user's mobile phone number, ID card number or unified social credit code. In Yiwu Tianxiang Medical Oriental Hospital v 19th Floor Network Co., Ltd., the court held that "as mobile phones have implemented real-name authentication and are easy to use and fully functional, mobile phone numbers can be used as a form of electronic identity authentication"[13]. This means that in the context of Chinese law, a user's mobile phone number can be clearly linked to the personal identity of the user of the number, in other words, this number information is personal information with direct identification properties at the legal level. So, the internet platforms such as Sina Weibo, Douyin, Today's Headlines, WeChat (Public) and Xiaohongshu, which have made their users' IP attribution information public since this year, not only have this information but also *de facto* hold the real identity information of users who post or leave comments. As mentioned above, such real identity information is personal information that China's PIPL recognises and protects.

Taken together, for these platforms, although the identity or characteristics of the information subject cannot be directly identified solely based on IP attribution information, they can accurately correspond the disputed information to the specific information subject by combining it with the real identity information that the user must provide when registering, to reach the vertical counterpart requirement. At the same time, because the real identification of the user's information is so highly identifiable and has been clearly limited to specific individuals, it also meets the requirement of differentiation in terms of horizontal elements and will not be confused with other information subjects. It is a superficial fact that IP attribution information can be combined with other information to accurately identify the subject of this information, and this clear and concise indirect identification is one of the dimensions of identification explicitly governed by China's PIPL.

It is therefore concluded that IP attribution information can be covered by the term "personal information" in the context of China's PIPL and that, as a result, user subjects can protect their personal information rights under this law.

5. Conclusion

In China, the trend in the regulation of the handling of personal information is that legislation on personal information protection is being implemented, en-

[13] Yiwu Tianxiang Medical Oriental Hospital v 19th Floor Network Co., Ltd. (2018) Zhe 0782 Min Chu No. 9873.

forcement is being tightened, and the responsibility of platforms is being reinforced. It is foreseeable that the reveal of IP attribution information will most likely be implemented on more platforms, and other measures beyond this feature will also be explored on a trial basis. From this perspective, the findings of this article are of both theoretical and practical importance. First, for the key concept that is left blank and ambiguous, this paper provides a general approach to clarify how the concept is interpreted and applied, which can help to enhance legal certainty, predictability and operability. Secondly, this paper shows how to determine the applicability of China's PIPL for non-statutory categories of information, which realistically responds to the concerns of IP attribution information subjects regarding the safeguarding of their personal information rights. In the longer term, the methodological refinements and application examples in this article on identifiability term and identification criteria can also be applied to solve related problems in the future.

Specifically, the disclosure of IP attribution information raises concerns about the protection of personal information, starting from the fact that this information does not fall within the categories of personal information explicitly covered by China's PIPL. In a general sense, the Law only protects personally identifiable information without a clear definition of "identifiability". This article addresses this issue from two perspectives. Firstly, given that the legal meaning of the term identifiability is uncertain, this article begins by reading the term on three levels to explain as comprehensively as possible what personally identifiable information the PIPL is intended to govern. On this basis, to enhance the certainty and operability of the identifiability criterion, this paper attempts to distil two constituent elements of this criterion, namely the horizontal distinction (between different subjects of information) and the vertical counterpart (between the disputed information and that subject of the information), which must be satisfied simultaneously. By analysing the usual approach of Chinese courts to this issue, and drawing on the experience and lessons learned from relevant foreign judicial cases, this article further suggests that a subjective/relative approach is more appropriate in determining the vertical relevance of the personal information identification criteria under China's PIPL. On this basis, this article answers the current general public concern and affirms that IP attribution information is personal information in the context of China's PIPL. As a result, users of various internet service provision platforms may be protected by the PIPL in their personal information rights when their IP attribution information is made public.

Of course, this is not the end of the controversy. The question that remains to be explored is, what is the basis for the legality of these internet platforms revealing users' IP attribution information? Does this data processing comply with Article 13 of China's PIPL? The answers to these questions are crucial, as they will determine whether this processing by these platforms is legally permissible and will ultimately affect whether the platforms will be held liable for it. From another perspective, the lawful basis clause for the processing of information on platforms can be seen as an important window into how legislators have balanced the interests and values of platform regulation and personal information protection. However, the answers to these questions are not obvious and require in-depth and careful further analysis in the context of recent Chinese legislation.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

Aoligei Say (2022, May 6). *Why did Ma Make a Mess? Why Is the IP Going Public? Be Wary of the Trap of Subverting the State*. https://www.163.com/dy/article/H6NF7JQM0552YQ30.html

Article 29 Data Protection Working Party (Art. 29 WP) (2007). *Opinion 4/2007 on the Concept of Personal Data* (01248/07/EN. (2007)). https://www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf

Bygrave, L. A., & Tosoni, L. (2020). Article 4.1. In C. Kuner, L. A. Bygrave, & C. Docksey (Eds.), *The EU General Data Protection Regulation (GDPR): A Commentary* (pp. 103-115). Oxford University Press.

Cao, B. (2022). Reflection and Reconstruction on the Interpretation Path of Personal Information Identifiability. *Administrative Law Review, 4,* 133-144.

Cheng, J. F. (2008). The Role of MAC and IP Addresses in Computer Networks. *Science and Technology of West China, 7,* 26-27+53.

Gao, F. (2021). Personal Information Processing: The Object of the China's Personal Information Protection Act. *Studies in Law and Business, 38,* 73-86.

Garfinkel, S. L. (2015). *De-Identification of Personal Information* (NIST IR 8053). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8053

He, J. (2022, April 30). *Are You Afraid when IP Attribution Information Are Revealed?* https://baijiahao.baidu.com/s?id=1731484009244110667&wfr=spider&for=pc

Leenes, R. E. (2007). Do They Know Me? Deconstructing Identifiability. *University of Ottawa Law and Technology Journal, 4,* 135-161.

Li, B. C., Xiong, Y., Huang, T., & Pan, L. (2020). Simulation-Deduction Model and System Construction of Intelligent Guidance of Network Public Opinion. *National Defense Technology, 41,* 35-40.

Liu, Y. P., & Lu, Z. X. (2002). Limitation in Binding MAC and IP. *Application Research of Computers, 9,* 83-85.

Niemann, F., & Schuessler, L. (2016, October 21). *CJEU Decision on Dynamic IP Addresses Touches Fundamental DP Law Questions*. Bird & Bird. https://www.twobirds.com/en/insights/2016/global/cjeu-decision-on-dynamic-ip-addresses-touches-fundamental-dp-law-questions

Nissenbaum, H. (2018). Respecting Context to Protect Privacy: Why Meaning Matters. *Science and Engineering Ethics, 24,* 831-852. https://doi.org/10.1007/s11948-015-9674-9

Purtova, N. (2018). The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law. *Law, Innovation and Technology, 10,* 40-81. https://doi.org/10.1080/17579961.2018.1452176

Purtova, N. (2022). From Knowing by Name to Targeting: The Meaning of Identification under the GDPR. *International Data Privacy Law, 12,* ipac013.

https://doi.org/10.1093/idpl/ipac013

Qi, A. M., & Zhang, Z. (2018). Identification and Reidentification: The Definition of Personal Information and the Legislative Choice. *Journal of Chongqing University (Social Science Edition), 24,* 119-131.

Ren, X., & Wang, Y. M. (2020). Research on the Dilemma and Countermeasures after the Real-Name System of the Whole Network. *Hubei Social Sciences, 4,* 155-163.

Su, L. (1997). Difficulties of Interpretation: The Pursuit of Several Approaches to the Interpretation of Legal Texts. *Social Sciences in China, 4,* 11-32.

Wang, J. (2022). Digital Citizen Ethics: New Approaches to the Governance of Cyber Violence. *ECUPL Journal, 25,* 28-40.

Wang, L. M., & Ding, X. D. (2021). On the Highlights, Characteristics and Application of Personal Information Protection Law. *The Jurist, 6,* 1-16+191.

Wen, J. B., & Xiao, D. M. (2022). Definition of Personal Whereabouts Information in China: Dilemma and Way-Out. *Library Tribune, 42,* 55-64.

Wu, C. H. (2022). *Data Jurisprudence*. Law Press.

Xie, H. (2015). On the Customary Basis for the Creation of New Rights. *Studies in Law and Business, 32,* 44-53.

Yu, J., & Ye, M. T. (2018). Definition and Management of Malware. *Journal of Zhejiang University of Technology (Social Science), 17,* 418-424.

Zhao, J. W. (2021). The Dilemma of Applying the "Identifiability" Standard to Personal Information and Theoretical Correction: The Example of Used Car Condition Information. *Journal of Social Sciences, 12,* 126-135.