CHINA LAW UPDATE

A BALANCE BETWEEN SOCIAL MEDIA USERS' PERSONAL INFORMATION PROTECTION AND COMBATING (MIS) AND (DIS)INFORMATION IN CHINA*

Fan Jinghe**

Tang Wenhan***

Table of Contents

* We are grateful to Professor Cheng Xiao and the TCLR editors for their valuable comments on aspects of this work.

** Fan Jinghe, DPhil in Law candidate at the University of Oxford.

*** Tang Wenhan, LL.M. at Duke University.

A BALANCE BETWEEN SOCIAL MEDIA USERS' PERSONAL INFORMATION PROTECTION AND COMBATING (MIS) AND (DIS)INFORMATION IN CHINA

Fan Jinghe

Tang Wenhan

I. INTRODUCTION

The emergence of social media platforms enables false information to spread much more rapidly and widely. Studies suggest that the number of (mis) and (dis)information on social media has increased exponentially in China during the past few years, particularly after the outbreak of Covid-19 Pandemic.[1] A proliferation of strategies has been proposed in China to diminish (mis) and (dis)information. One category is to impose legal liabilities or sanctions on persons that create or circulate false information.[2] Online platforms are also obliged to take down and report the false information that may disrupt social order and stability once they have found it.[3] If platforms fail to fulfill their obligations, public authorities could order them to make corrections, or even revoke licenses when the circumstances are serious.[4]

Another category focuses on improving transparency. Compared with retrospectively imposing legal sanctions, efforts to improve transparency aim to lessen the continuous impact of (mis) and (dis)information and lead the public to learn more about the truth. For example, multiple public authorities in China have registered their official accounts on social media platforms like Weibo.[5] They are able to check the fact and publish the verified news story

[1] *See* Shuo Tang, Lars Willnat & Hongzhong Zhang, *Fake News, Information Overload, and the Third-Person Effect in China*, 6 GLOBAL MEDIA & CHINA 492, 493 (2021); Niandu Chuanmei Lunli Yanjiu Ketizu (年度传媒伦理研究课题组), *2020 Xujia Xinwen Yanjiu Baogao* (2020年虚假新闻研究报告) [*2020 Annual Research Report on Fake News*], 1 XINWEN JIZHE (新闻记者) [JOURNALISM REV.] 23, 23 (2021).

[2] *See* Xing Fa (刑法) [Criminal Law] (promulgated by the Nat'l People's Cong., Jul. 1, 1979, rev'd Mar. 14, 1997, last amended Dec. 26, 2020, effective Mar. 1, 2021) art. 291 (I) para. 2, CLI.1.349391 (Chinalawinfo). According to Criminal Law Article 291 (I), the person who fabricates false information or knowingly spreads false information that seriously disturbs the social order might be sentenced to fixed-term imprisonment of no more than three years; if the circumstances are extremely severe, the person shall be sentenced no less than three years but no more than seven years.

[3] *See* Wangluo Anquan Fa (网络安全法) [Cybersecurity Law] (promulgated by the Standing Comm. Nat'l People's Cong., Nov. 7, 2016, effective Jun. 1, 2017) art. 47, CLI.1.283838 (Chinalawinfo); Hulianwang Xinxi Fuwu Guanli Banfa (互联网信息服务管理办法) [Regulation on Internet Information Service] (promulgated by St. Council, Sep 25, 2000, rev'd Jan. 8, 2011, effective Jan. 8, 2011) arts. 15(6) and 16, CLI.2.174868 (Chinalawinfo).

[4] *See Regulation on Internet Information Service*, *supra* note 3, art. 23.

[5] For example, information offices of different provinces have registered official accounts to release policies and instant responses to high-stake events. *See e.g.*, Beijing Fabu (北京发布), https://weibo.com/bjfbt (last visited Jul. 27, 2022); Shandong Fabu (山东发布), https://weibo.com/shandongfabu (last visited Jul. 27, 2022). Some provinces have also established fact-checking accounts, such as Shanghai Piyao Pingtai (上海辟

once they have found (mis) and (dis)information. Some digital platforms in other countries may work with third parties who are members of the Poynter International Fact-Checking Network to identify the false stories.[6] In addition, platforms could flag disputed stories and offer "related articles" beneath the disputed information so that readers could think critically. "Instead of killing the story, surround[ing] the story with related articles could provide more context and alternative views to readers."[7]

Disclosing social media users' personal information is proposed to be another solution to promote transparency. By requiring social media users to disclose their real identities or location to the public, some policies or platforms attempt to help the public to clarify the potential sources of publishers behind pseudonymous accounts. In October 2021, the Cyberspace Administration of China ("CAC", 国家互联网信息办公室) released the draft of the *Provisions on Management of Internet Users' Account Information* ("the *Provisions*") for public consultation.[8] In the draft, Article 12 intended to require all internet information service providers to display users' IP territoriality on the account information pages prominently.

IP territoriality refers to the geographical location extracted from an IP address of an individual's or a party's device.[9] The technology of IP geolocation can assist websites operators in obtaining users' geographical location by comparing IP addresses with geolocation databases owned by geolocation service providers.[10] The most common geographical information that websites can obtain through IP addresses is country, region, city, or time zone. Websites may also have access to the postal code, approximate latitude and longitude, or even the relevant organisation attached to the device (e.g., with the domain name ".edu"). Whenever we visit a website using our own device, our IP address is automatically shared with the website. Consequently, internet information service providers already possess the IP address of our device and can extract the geolocation associated with the IP address.[11]

According to the draft, however, what makes Article 12 unique is the requirement of disclosing users' IP territoriality to the public. According to the

---

谣平台), https://weibo.com/u/7751952906?refer_flag=1005055013_&ssl_rnd=1658927949.9416 (last visited Jul. 27, 2022).

[6] *See* Casey Newton, *Facebook Partners with Fact-Checking Organizations to Begin Flagging Fake News*, THE VERGE (Dec. 15, 2016), https://www.theverge.com/2016/12/15/13960062/facebook-fact-check-partnerships-fake-news.

[7] Alberto Alemanno, *How to Counter Fake News? A Taxonomy of Anti-Fake News Approaches*, 9 EUR. J. RISK REG. 1, 4 (2018).

[8] Hulianwang Yonghu Zhanghao Mingcheng Xinxi Guanli Guiding (Zhengqiu Yijiangao) (互联网用户账号名称信息管理规定(征求意见稿)) [Provisions on the Administration of Internet Users' Account Name Information Administration (Draft for Comment)], CYBERSPACE ADMINISTRATION OF CHINA (Oct. 26, 2021), http://www.cac.gov.cn/2021-10/26/c_1636843202454310.htm.

[9] *See* Jamie Taylor, Joseph Devlin & Kevin Curran, *Bringing Location to IP Addresses with IP Geolocation*, 4 J. EMERGING TECH. IN WEB INTELLIGENCE 273, 273–74 (2012).

[10] *See id.*

[11] *See id.*

draft, for users within China, platforms will display the provinces reflected through users' IP addresses when users send the last message.[12] For users from overseas, the country of their IP addresses will be demonstrated. This measure is aimed at preventing users from being misled by publishers who pretend to be witnesses of high-stakes events or local people familiar with affairs in specific regions.[13]

Since April 2022, before the draft of the *Provisions* was amended and formally enacted, Weibo had started to display existing users' IP territoriality without obtaining their consent. Users' IP territoriality was shown next to their usernames not only on their information pages but also in each post and comment published by users.[14] Following Weibo, multiple major online platforms, such as Zhihu, Xiaohongshu, Douyin, Wechat, and Bilibili, adopted the same approach of disclosing users' IP territoriality.[15]

Nevertheless, this draft and the changes in platforms' information policies raised heated discussions. Internet users could entail both individuals and institutions.[16] Due to its compulsory nature, whilst the disclosure aims at helping promote transparency of the sources of online posts and comments, it is likely in tension with individual users' personal information protection. This seems particularly controversial after the *Personal Information Protection Law* ("PIPL") was enacted on August 20, 2021.[17]

On June 9, 2022, the *Provisions* were officially adopted.[18] Distinct from the draft, the binding text stipulates that "an Internet information service provider shall display information on the territoriality of the Internet Protocol (IP) address of an Internet user account within a reasonable range on the Internet user account information webpage, so that the public may supervise for the public interest." The binding text does not clarify which specific level of region users' IP territoriality should be disclosed. Moreover, the disclosure

[12] *See* the *Provisions* (Draft for Comment), *supra* note 8, art. 12.

[13] *See* Weibo Guanliyuan (微博管理员) [Weibo Administrator], *IP Shudi Gongneng Shengji Gonggao* (IP属地功能升级公告) [*IP Territoriality Function Update Announcement*] (Apr. 28, 2022), https://weibo.com/1934183965/LqvYeCdBu (last visited May 30, 2023).

[14] *See id.*

[15] *See* Dianshang Bao (电商报) [E-Commerse News], *Douyin, Kuaishou, Xiaohongshu Deng Pingtai Jiang Xianshi IP Shudi* (抖音、快手、小红书等平台将显示IP属地) [*Platforms such as Douyin, Kuaishou, and Xiaohongshu will Display IP Territoriality*], WANG YI (网易) (Apr. 19, 2022), https://www.163.com/dy/article/H5ABVO850514CA4V.html (last visited May 30, 2023).

[16] *See* the *Provisions* (Draft for Comment), *supra* note 8, art. 7.

[17] Guanyu Zhonghua Renmin Gongheguo Geren Xinxi Baohufa Cao'an De Shuoming (关于《中华人民共和国个人信息保护法(草案)》的说明) [Explanation on the Draft Personal Information Protection Law of the People's Republic of China] (Aug. 20, 2021) [hereinafter "*Explanation*"], http://www.npc.gov.cn/npc/c30834/202108/fbc9ba044c2449c9bc6b6317b94694be.shtml (last visited Jul. 27, 2022); Geren Xinxi Baohu Fa (个人信息保护法) [Personal Information Protection Law] (promulgated by the Standing Comm. Nat'l People's Cong., Aug. 20, 2021, effective Nov. 1, 2021), CLI.1.5055321 (Chinalawinfo).

[18] Hulianwang Yonghu Zhanghao Xinxi Guanli Guiding (互联网用户账号信息管理规定) [Provisions on the Administration of Internet Users' Account Name Information Administration] (promulgated by the Cyberspace Administration of China, Jun. 27, 2022, effective Aug. 1, 2022) (hereinafter "the *Provisions*"), http://www.cac.gov.cn/2022-06/26/c_1657868775042841.htm.

is limited to on the "account information page" "within a reasonable scope" to "facilitate the public supervision for the public interest". These amendments indicate that the *Provisions* recognized it is not feasible to provide a universally applicable standard and the specific context of disclosure needs to be taken into consideration. The binding text also leaves more discretion to online platforms to determine whether and how should users' IP territoriality be disclosed.

Against this backdrop, it seems that different platforms' practices still vary, and there is no sufficient evidence showing that they have altered their practice responding to the requirement of "reasonable scope." Those controversial debates may still exist surrounding a range of questions: Is users' IP territoriality personal information? Which legal basis is relied upon when online platforms disclose users' IP territoriality without obtaining their consent before the *Provisions* were enacted? According to the purpose stated in the binding text, how should we look into the balance between personal information protection and the public interest behind addressing (mis) and (dis)information?

This Note attempts to respond to these challenges. By examining the PIPL Article 4, Part II will analyze why users' IP territoriality may fall within the scope of personal information. Part III will discuss if there is any legal basis apart from information subjects' consent that could justify the disclosure of users' IP territoriality with the aim of addressing (mis) and (dis)information. This part will narrow down to the legal basis in the PIPL Article 13 Paragraph 1(5) – processing personal information "within a reasonable scope" to conduct "news reporting, public supervision, or other activities in the public interest". Part IV attempts to clarify the meaning of "reasonable scope" in the PIPL Article 13 Paragraph 1(5) which plays a significant role in balancing between personal information protection and public interests. This part will borrow insights from the considerations of proportionality, fundamental principles in the PIPL, and the regime of personal information impact assessment to refine the analytical framework for online platforms to reconcile these competing rights and interests. By using IP territoriality as an example, we will apply this framework in the context of combating (mis) and (dis)information. Part V will conclude all of our arguments.

Before moving on, it is necessary to notice some caveats. First, the Note will particularly focus on social media platforms due to their ability to let everyone publish and share content with fast speed and intense audience engagement. These features make social media platforms unique from other types of internet services, such as search engines or news information services, which are also within the broad scope of the *Provisions*.[19]

Second, the Note will use IP territoriality as a prominent example to show how new solutions of eliminating (mis) and (dis)information and embedded

[19] *See* the *Provisions* Article 23. In the *Provisions*, internet information service providers are defined very broadly as "designed to provide users with internet information release and application platform services." This definition includes but is not limited to news information services, online publishing services, search engines, instant messaging, interactive information services, live streaming, apps, and software downloads.

public interests come into conflict with users' personal information protection. According to the *Provisions*, IP territoriality is not the only type of information that needs to be displayed (e.g., Article 11 of the *Provisions*).[20] However, this provision is optional and will only affect those who actively participate in the information production of a specific area.

Lastly, it is essential to define (mis) and (dis)information. Disinformation is the deliberate fabrication or dissemination of false facts which may mislead, deceive, or harm the public.[21] Related but different, misinformation is false content shared by a person who does not realize its falsity with no malicious purposes.[22] Both (mis) and (dis)information refer to factual statements that are verifiable and inaccurate.[23] As suggested at the beginning, one's subjective intent behind disseminating false information may affect the result of the legal liability.[24] Nevertheless, in light of the unique characteristics of social media, such as the sheer number of users, instant spreading speed, and personalized content, false information will not always be prevented through penalizing specific perpetrators who create disinformation. Instead, incorporating mis-information into the scope of regulation may better reflect those measures of enhancing transparency of online posts' origins by lessening the dissemination of false information regardless of users' subjective intent. In addition, false information may include slanders which may infringe specific entities' rights of reputation. Relevant legal assessment of slanders will be outside the scope of this note. This note will thus use (mis) and (dis)information to represent all false information that may disturb the social order or harm the public.[25]

[20] Article 11 of the *Provisions* requires users who "choose to" engage in the production of information related to the economy, education, health care, and other areas to provide professional qualifications and background to service providers for verification. Their information of professional background is required to be displayed on the account information page as well.

[21] *See* Wayne Unger, *How the Poor Data Privacy Regime Contributes to Misinformation Spread and Democratic Erosion*, 22 SCI. & TECH. L. REV. 308, 311 (2021).

[22] *See* Kai Shu et al., *Mining Disinformation and Fake News: Concepts, Methods, and Recent Advancements*, *in* DISINFORMATION, MISINFORMATION, AND FAKE NEWS IN SOCIAL MEDIA: EMERGING RESEARCH CHALLENGES AND OPPORTUNITIES 1, 2–3 (Kai Shu et al. ed., 2020).

[23] *See* Wang Jian (王剑), Wang Yucui (王玉翠) & Huang Mengjie (黄梦杰), *Shejiao Wangluo Zhong De Xujia Xinxi: Dingyi, Jiance Ji Kongzhi* (社交网络中的虚假信息: 定义, 检测及控制) [*False Information in Social Networks: Definition, Detection, and Control*], 48 JISUANJI KEXUE (计算机科学) [COMPUTER SCI.] 263, 264 (2021); Liu Hailong (刘海龙) & Yu Ying (于瀛), *Gainian De Zhengzhi Yu Gainian De Lianjie: Yaoyan, Chuanyan, Wudao Xinxi, Xujia Xinxi Yu Jiaxinwen De Gainian De Chonggou* (概念的政治与概念的连接: 谣言、传言、误导信息、虚假信息与假新闻的概念的重构) [*Bridging Concepts: The Politics of Concepts and Conceptual Reconstruction of Yaoyan, Rumor, Disinformation, Misinformation, and Fake News*], 12 XINWENJIE (新闻界) [PRESS CIRCLES] 23, 31–32 (2021).

[24] *See* Xing Fa (刑法), *supra* note 2, art. 291 (I) para. 2.

[25] Fake news is frequently used to represent similar meanings. It is worth noting that, however, providers of internet news information services are required to get permission from public authorities in China. Per the *Provisions for the Administration of Internet News Information Services* (互联网新闻信息服务管理规定, 2017) Article 6, entities who can collect, edit, and issue news services are also limited. Compared with fake news, (mis) and (dis)information may demonstrate the diversity of publishers in social media.

II. THE LEGAL NATURE OF THE INFORMATION THAT HAS BEEN DISCLOSED FOR COMBATING (MIS) AND (DIS)INFORMATION

The primary source of the regulatory framework for disclosing personal information to combat (mis) and (dis)information is the PIPL. Implemented in 2021, the PIPL was enacted to "protect rights and interests relating to personal information, regulate personal information processing activities, and promote the reasonable use of personal information (Article 1). Per PIPL Article 4, disclosure is one type of personal information processing activity.[26] It is thus compulsory for personal information processors to conform with PIPL if the information they disclose is not anonymized (Article 73) and is related to identified or identifiable natural persons (Article 4 Paragraph 1).

Since multiple platforms initiated measures to disclose users' information (e.g., IP territoriality) adjacent to their account name, some have argued that the disclosed information is not personal information; therefore, the measures are not subject to the regulation of PIPL. For instance, some suggest that IP territoriality cannot identify specific natural persons as it could merely reflect the province where millions of people may locate simultaneously.[27] It is also hotly debated whether users' information falls within the scope of PIPL if it is displayed without being tied to users' real names.[28] These arguments remind us to review the definition of personal information and examine the legal nature of the information that may be disclosed for combating (mis) and (dis)-information.

In PIPL Article 4, personal information covers "all kinds of information related to identified or identifiable natural persons that are electronically or otherwise recorded, excluding information that has been anonymized." This definition raises four basic elements: (i) all kinds of information; (ii) related to; (iii) identified or identifiable; (iv) natural person. As this Note focuses on the protection of users who are natural persons, our following analysis will primarily discuss two elements that might be more controversial: "identifiability" and "related to."

[26] According to PIPL Article 4 Paragraph 2, "personal information processing includes, but is not limited to, the collection, storage, use, processing, transmission, provision, disclosure, and deletion of personal information." In this Note, we will primarily focus on the disclosure of personal information. However, the framework of balancing test and relevant considerations could be used for other types of processing activities in the context of combating (mis) and (dis)information.

[27] See *Xianshi IP Shudi Hui Xielu Geren Xinxi Ma?* (显示IP属地会泄漏个人信息吗?) [*Will Displaying IP Territoriality Disclose Personal Information?*], ZHONGGUO JINGJIWANG (中国经济网) [CHINA ECONOMIC NET] (Jul. 10, 2022), https://www.piyao.org.cn/2022-06/16/c_1211657346.htm (last visited Jul. 27, 2022).

[28] *See* Frederik Borgesius, *Singling out People Without Knowing Their Names – Behavioural Targeting, Pseudonymous Data, and the New Data Protection Regulation*, 32 COMPUTER L. & SECURITY REV. 256, 267–270 (2016).

A. *Definitions of Personal Information*

1. "identified or identifiable natural person." Personal information should be associated with an "identified or identifiable" natural person. One person is identified when he or she could be directly distinguished from all others through the piece of information in question. Direct identification is basically achieved through certain "identifiers" which are specific to one's physical, physiological, economic, cultural, or social identity, such as identification numbers and fingerprints.[29] Indirectly identifiable information, however, is normally not tied to the real name of individuals. Notwithstanding, indirectly identifiable information can be used to single out information subjects combined with other information on categorical levels, such as age, gender, regional origins, etc.[30] With the exponential development of big data and analytics technology, people can combine indirectly identifiable information from different datasets to tie a direct identifier to nameless data or create new information about individuals.[31] Notably, not showing real names is distinguished from anonymization (PIPL Article 73(4)). Anonymization would render information subjects unidentifiable from certain information and make the information unrestorable (PIPL Article 73(4)). If one piece of information could still enable identification of specific natural persons with the support of additional information, it is still indirectly identifiable personal information and will be subject to the protection of PIPL (PIPL Article 73(3)).

The assessment of indirect identifiability is conducted contextually so as to achieve a balance between the need of protecting data subjects and the re-use of information.[32] According to academic interpretation and comparative law, relevant contextual factors may include purposes, methods of processing, the available technology of identification at the time of processing, the costs and the amount of time required for identification, etc.[33]

Here it is worth probing from whose perspective the possibility of identification ought to be assessed. In recent jurisprudence of personal information protection in China, the Beijing Internet Court held that disclosure of personal

[29] *See* Xinxi Anquan Jishu Geren Xinxi Qubiaoshihua Zhinan (信息安全技术 个人信息去标识化指南) [Information Security Technology—Guide for De-identifying Personal Information] (promulgated by State Admin. for Market Regulation & Standardization Admin. of China, Aug. 30, 2019, effective Mar. 1, 2020), art. 3.7.

[30] *See* CHENG XIAO (程啸), GEREN XINXI BAOHUFA LIJIE YU SHIYONG (个人信息保护法理解与适用) [THE UNDERSTANDING AND APPLICATION OF PERSONAL INFORMATION PROTECTION LAW] 62 (2021).

[31] *See* GEREN XINXI BAOHU FA TIAOWEN JINGJIE YU SHIYONG ZHIYIN (个人信息保护法条文精解与适用指引) [DETAILED EXPLANATION AND APPLICATION GUIDELINE TO THE PERSONAL INFORMATION PROTECTION LAW] 52 (Zhou Hanhua (周汉华) ed., 2022). *See also* Manon Oostveen, *Identifiability and the Applicability of Data Protection to Big Data*, 6 INT'L DATA PRIVACY L. 299, 307 (2016).

[32] *See id.*, at 52.

[33] *See* the General Data Protection Regulation ("GDPR"), Recital 26. *See also* Zhao Jingwu (赵精武) *Geren Xinxi Keshibie Biaozhun De Shiyong Kunju Yu Lilun Jiaozheng* (个人信息"可识别"标准的适用困局与理论矫正) [*The Application Predicament and Theoretical Correction of "Identifiability" of Personal Information*], 12 SHEHUI KEXUE (社会科学) [J. SOC. SCI.] 126, 135 (2021).

information should not be assessed in isolation, but in combination with relevant information possessed by the information processor in specific circumstances.[34] According to the court, it is primarily crucial to examine whether information processors possess the combination of different datasets that would enable identification. This is because the processors are duty-bearers of PIPL. If the information is identifiable, they are mandated to conform to the basic principles and obligations of PIPL to ensure the lawfulness and safety of processing activities for the entire cycle. Otherwise, there would be a significant loophole for platforms to arbitrarily process any information related to users other than direct identifiers without fulfilling any obligations of impact assessment and reducing potential risks on information subjects.

At the same time, when analyzing the nature of information, it is also important to consider the available technology of re-identification that any third parties may access. This is particularly the case when information is released publicly. Even if the processors have removed direct identifiers, they are still required to consider whether there is any residual risk of re-identification from third parties that could reasonably be expected after the disclosure. This is first because the potential harm to information subjects can result from processing activities, even if the individual's name or other direct identifiers have not been tied to the information. For example, behavioral targeting aims to "deliver the right ad to the right person at the right time."[35] Whilst it seems that profiles and ads are customized for a technical account, it is a natural person who has been affected by the content of ads or profiles. Here the third party would not care about users' real names or ID numbers, but whether users will receive and be affected by that piece of information.[36] Similarly, online discrimination, fraud, and harassment, can all happen without knowing the real name of the information subjects. Moreover, in different circumstances, potential third parties may include not only the general public, but also entities that are able to conduct big data analytics. A criterion of assessment that exclusively considers the perspective of information processors or ordinary people would arbitrarily ignore third parties who might have access to other datasets and put information subjects at risk.[37] Therefore, combined with contextual factors suggested above, if either information processors or any third parties could reasonably

[34] *See* Ling Moumou Su Beijing Weibo Shijie Youxian Gongsi (凌某某诉北京微播视界有限公司) [Ling Moumou v. Beijing Weibo Shijie Co., Ltd.] ((2019)京0491民初6694号, Beijing Internet Ct., July 30, 2020).

[35] Borgesius, *supra* note 28, at 268.

[36] *See id.*

[37] *See e.g.*, Han Xuzhi (韩旭至), *Geren Xinxi Gainian De Fa Jiaoyi Xue Fenxi* (个人信息概念的法教义学分析) [*The Concept of Personal Information in Legal Dogmatics Angle*], 2 CHONGQING DAXUE XUEBAO (SHEHUI KEXUE BAN) (重庆大学学报(社会科学版)) [J. CHONGQING UNIV. (SOC. SCI. ED.)] 154, 159–60 (2018).

likely identify a natural person, the information should be considered as identifiable.[38]

Applying the above interpretation, in the context of disclosing social media users' information, we would argue that IP territoriality is identifiable information from the perspectives of both information processors and third parties. As regards information processors, in 2019, the Beijing Internet Court found that the information of personal location, no matter precise or obscure, should be considered personal information if it is combined with phone numbers that can directly identify individuals.[39] Individuals are mandated to provide true identity information (including real names and ID numbers) to register for mobile phone numbers and all other Internet services per the *Cybersecurity Law* Article 24. This further indicates that each phone number and social media account is connected to only one specific individual, though an individual could have multiple phone numbers or accounts. Therefore, from the perspective of social media platforms, which are information processors, the unique combination of IP territoriality and other direct identifiers (e.g., phone numbers, ID numbers) would enable every account user to be identified.

Third parties may also identify information subjects when they combine users' IP territoriality with other information, depending on the available datasets and technology. From the outset, among at least millions of users, not all of them choose to use pseudonyms. Users who showcase real names may be confronted with new risks due to the mandatory disclosure of more personal information. Also, not showing real names could only lower, but not eliminate the potential harm to social media users. Techniques to re-identify information subjects continue to improve. In 2006, search engine provider AOL released a data set of nameless search profiles, each tied to a random number. Within a few days, several journalists had found one of the searchers: an elderly woman with a dog, from the town of Lilburn. An interview confirmed that the journalists had correctly identified her.[40] The methods of disclosing further increase the possibility of identification. In social media platforms, users' IP territoriality is demonstrated alongside the username and all other information that has been voluntarily published by users, including details about daily lives, photographs, etc. These pieces of information could be accessed by anyone unless users set restrictions. Third parties who have stronger technological capabilities than the public, such as data analytics companies and law enforcement agencies, are more likely to identify natural persons through these disclosed profiles or combine them with extra datasets. Therefore, it is still reasonably likely for third parties to identify the natural person, particularly

[38] *See* ZHONGHUA RENMIN GOUNGHEGUO GEREN XINXI BAOHU FA SHIYI (中华人民共和国个人信息保护法释义) [AN INTERPRETATION ON THE PERSONAL INFORMATION PROTECTION LAW OF THE PEOPLE'S REPUBLIC OF CHINA] 16 (Long Weiqiu (龙卫球) ed., 2021).

[39] *See* Ling Moumou v. Beijing Weibo Shijie Co., Ltd., *supra* note 34.

[40] *See* Michael Barbarom & Tom Zeller Jr., *A Face Is Exposed for AOL Searcher No. 4417749*, N.Y. TIMES (Aug. 9, 2006), www.nytimes.com/2006/08/09/technology/09aol.html (last visited Jul. 27, 2022).

when there is no technical limitation on third parties' access to information that has been disclosed.

In conclusion, from the perspective of both information processors and third parties, the mandatorily disclosed users' personal information, including the IP territoriality, should be considered identifiable.

2. "related to." Since indirectly identifiable information has a tendency to include more personal information into the protection of PIPL, the requirement of "related to" aims to narrow the scope of personal information by examining links between the information in question and the individual. In general, when the information processor has already known the identity of a natural person, the information that is restored in one's personal records will be easily considered as related to that natural person.[41] Notwithstanding, in some circumstances, it would be more complex to demarcate the boundary between personal data and non-personal data. PIPL does not elaborate so much on the scope of "related to." In the GDPR, whose definition of personal information is mostly similar to that of PIPL, personal information is "related to" an individual when its content is about the person, the purpose of processing is to influence or evaluate the person, or the result of processing activities have an impact on the person. Notably, when some information concerns objects that are associated with someone, such as houses or mobile cars, it is imperative to examine how the information is used.[42] This approach could reasonably exclude information that may belong to the public sphere. For example, if the value of a car is merely used to reflect the average price of a specific type in the market, it may not be related to its owner. If the value assessment is intended to determine the taxes one is going to pay, it may be related to its owner.[43]

Applying this interpretation, social media users' IP territoriality should be considered as related to corresponding social media users under PIPL. To start with, social media users' IP territoriality is extracted from the IP address sent to social media platforms automatically from users' devices when they post and comment.[44] The content of the information is related to the user by reflecting users' real-time location at the level of countries or provinces. Though in some circumstances, users may access the internet through public computers rather than their own devices, the disclosure of IP territoriality is aimed at helping the public know where a specific user is located, and will leave the impression that the user stays in the region demonstrated by the IP territoriality, regardless of

[41] *See* ZHONGHUA RENMIN GONGHEGUO GEREN XINXI BAOHUFA SHIYI (中华人民共和国个人信息保护法释义) [AN INTERPRETATION ON THE PERSONAL INFORMATION PROTECTION LAW OF THE PEOPLE'S REPUBLIC OF CHINA] 22 (Yang Heqing (杨合庆) ed., 2021). *See also* LONG, *supra* note 38, at 15–16; CHENG, *supra* note 30, at 57–58.

[42] *See* Zhao, *supra* note 33, at 134.

[43] *See* Article 29 Data Protection Working Party, *Opinion 4/2007 on The Concept of Personal Data* (Jun. 20, 2007) [hereinafter "A29WP, *Opinion 4/2007*"], at 9–10, EUROPEAN COMMISSION, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf.

[44] *See* Weibo Administrator, *supra* note 13.

its reliability. More importantly, users' IP territoriality will renew every time people use their accounts. The track of IP territoriality over the long time span will form a specific dataset connected to the account of a specific natural person. For social network accounts owned and used by natural persons, therefore, IP territoriality that is disclosed should be deemed as specifically related to users behind social network accounts.

B. Summary

In short, in this part we argue that disclosing users' information without showing their real names does not satisfy the standard of anonymization in PIPL. Rather, the disclosed information, such as IP territoriality, is related to an indirectly identifiable natural person behind the account and thus falls within the scope of personal information as per the PIPL Article 4. It is a better option not to unduly restrict the concept of personal information but rather to note that there is certain flexibility in the rules of processing personal information.[45] The broader scope of personal information is intentionally designed for enhancing protection and integrating procedural safeguards within the PIPL in the whole lifecycle of processing personal information from determining whether to initiate processing or not.[46] In particular, like what is indicated in the *Provisions* Article 12, when all Internet information service providers start to implement the same policy of disclosing users' IP territoriality, there is little room left for individual users to protect themselves if the definition of personal information is excessively narrowed. As illustrated in Part III, the task of balancing between competing different rights and interests in this context should be left to the rigorous framework of the PIPL.

III. THE LEGAL BASIS FOR PROCESSING PERSONAL INFORMATION FOR THE PURPOSE OF COUNTERING (MIS) AND (DIS)INFORMATION

According to PIPL Article 13, data processors must obtain information subjects' consent (Article 13 Paragraph 1(1)) to disclose their personal information unless one of the exceptions in paragraphs 1(2) to 1(7) are satisfied.[47] Since a platform's policy of disclosing users' IP territoriality is not aimed at contract performance or human resources management, it may not fit in Article 13 Paragraph 1(2). Also, as a continuous policy, disclosing personal infor-

[45] *See* A29WP, *Opinion 4/2007*, *supra* note 43, at 5.

[46] *See Explanation*, *supra* note 17.

[47] Apart from individual consent, according to the PIPL Article 13 Paragraphs 1(2) to 1(7), the processing is lawful when it is (i) necessary for the conclusion of a contract or for conducting human resource management (Paragraph 1(2)); (ii) necessary for fulfilling statutory functions or statutory obligations (Paragraph 1(3)); (iii) necessary for responding to public health emergencies or protect natural persons' life, health, or property safety in emergencies (Paragraph 1(4)); (iv) processed within a reasonable scope to conduct news reporting, public opinion-based supervision, or other activities in the public interest (Paragraph 1(5)); (v) the personal information that has been disclosed by the individuals themselves or legally disclosed reasonably (Paragraph 1(6)); (vi) under any other circumstances in any law or administrative regulation (Paragraph 1(7)).

mation to counter (mis) and (dis)information will not fall within the public health emergency exception of Article 13 Paragraph 1(4). To apply Article 13 Paragraph 1(6), the user must have disclosed the information to the public voluntarily or based on other legal bases prior to the processing activity in question. This legal basis relies on individual analyses of each user so that it could not provide a general exception for disclosing all social media users' information without previous consent.

Accordingly, we will focus on the other three potential legal bases to see whether they may justify mandating personal information disclosure for combating (mis) and (dis)information: statutory duties and obligations (PIPL Article 13 Paragraph 1(3)), specific circumstances in any other laws or administrative regulations (PIPL Article 13 Paragraph 1(7)), and public interest (PIPL Article 13 Paragraph 1(5)). As the first two exceptions are closely connected, we will discuss both of them in Section A.

A. Statutory Duties or Statutory Obligations

According to Article 13 Paragraph 1(3), when it is necessary to process personal information for the performance of statutory duties or statutory obligations, processors are not required to obtain information subjects' consent. "Statutory duties" refer to circumstances in which public authorities are obliged to process personal information based on legal provisions.[48] Any other entities may be mandated to collect personal information so as to fulfill "statutory obligations". According to the *Social Insurance Law* and the *Labor Contract Law*, for instance, employers should pay for work-related injury insurance.[49] In order to fulfill that obligation, employers could process employees' relevant personal information without obtaining employees' consent.

Before the *Provisions* were officially enacted, social media platforms could not rely on the previous draft as a resource for statutory obligations. Yet after the *Provisions* were passed, it remains open to debate whether departmental rules could impose statutory obligations on private entities to disclose personal IP territoriality in a reasonable scope to promote mass supervision and public interest.

According to the *Legislation Law* Articles 80 and 82, State Council departmental rules are not empowered to set out any requirements that impair the rights or increase the obligations of citizens, legal persons, and other organizations, unless laws or the administrative regulations, decisions, and orders of the State Council provide certain bases.[50] Some have also indicated

[48] *See* CHENG, *supra* note 30, at 130–33.

[49] *See* Shehui Baoxian Fa (社会保险法) [Social Insurance Law] (promulgated by the Standing Comm. Nat'l People's Cong., Oct. 28, 2010, rev'd Dec. 29, 2018, effective Dec. 29, 2018), art. 4, CLI.1.328179 (Chinalawinfo). *See also* Laodong Hetong Fa (劳动合同法) [Labor Contract Law] (promulgated by the Standing Comm.Nat'l People's Cong., Jun. 29, 2007, rev'd Dec. 28, 2012, effective Jul.1, 2013), art. 38, CLI.1.199310 (Chinalawinfo).

[50] *See* Lifa Fa (立法法) [The Law on Legislation] (promulgated by the Nat'l People's Cong., Mar. 15, 2000, rev'd Mar. 15, 2015, effective Mar. 15, 2015), CLI.1.245693 (Chinalawinfo).

that, according to the principle of legal reservations, when rights and interests of personal information protection are stipulated by the *Civil Code* and the PIPL, the legal norm which limits the right and interests of data subjects should also be at the same level of laws.[51] This interpretation could prevent state organs from expanding their own power and excessively processing personal information.[52] Though PIPL Article 62 does empower the national internet information administration to "develop specific rules and standards for personal information protection", the wording did not explicitly permit departmental rules to establish further limitations on data subjects' rights and interests. Importantly, Article 13 Paragraph 1(7) clearly negates the possibility for departmental rules to establish exceptions for information subjects' right to consent. A coherent and systemic interpretation of Article 13 would imply that provisions beneath the level of laws or administrative regulations could not set new legal bases through establishing statutory obligations. To conclude, it is difficult for Article 13 Paragraph 1(3) and Paragraph 1(7) to be appropriate legal bases for online platforms to disclose users' IP territoriality for the purpose of eliminating (mis) and (dis)information.

B. News Reporting, Media Supervision, and Other Activities Conducted for Public Interests

Without statutory obligations, information processors may rely on PIPL Article 13 Paragraph 1(5) when personal information is "reasonably processed for news reporting, public opinion supervision, and other activities conducted for public interest." News reporting involves discovering, organizing, editing, and disseminating facts and comments on social and public affairs. Per the *Provisions for the Administration of Internet News Information Services* Article 5, all news information services providers are obliged to be legally licensed.[53] By contrast, public opinion supervision is defined more broadly as supervision by the masses, which could be exercised by everyone in the era of social media.[54] Public opinion supervision originates from Articles 27 and 41 of the *Constitution of the People's Republic of China* (the "*Constitution*") which

[51] *See* Wang Xinxin (王锡锌), *Xingzheng Jiguan Chuli Geren Xinxi Huodong De Hefaxing Fenxi Kuangjia* (行政机关处理个人信息活动的合法性分析框架) [*An Analytical Framework for the Legitimacy of Personal Information Processing by Administrative Agencies*], 3 BIJIAO FA YANJIU (比较法研究) [J. COMP. L.] 92, 98–99 (2022).

[52] *See id.*, at 99.

[53] *See* Hulianwang Xinwen Xinxi Fuwu Guanli Guiding (互联网新闻信息服务管理规定) [Provisions for the Administration of Internet News Information Services] (promulgated by the Cyberspace Administration of China, May 2, 2017, effective Jun.1, 2017), CLI.4.293919 (Chinalawinfo).

[54] *See* Cheng Xiao (程啸), *Lun Woguo Minfadian Zhong De Geren Xinxi Heli Shiyong Zhidu* (论我国民法典中的个人信息合理使用制度) [*Research on the Fair Use of Personal Information in China's Civil Code*], 4 ZHONGWAI FAXUE (中外法学) [PEKING UNIV. L. J.] 1001, 1012 (2020).

stresses that all state organs must accept people's supervision and do their best to serve them.[55]

PIPL Article 13 Paragraph 1(5) is not the first rule which explicitly provides for the exception of journalism and public opinion supervision. Since 2020, the Civil Code Articles 999 and 1036 have both stipulated that individuals' names, portraits, and personal information can be reasonably used for news reporting and public opinion supervision with the aim of public interest. Both news reporting and public opinion supervision primarily intend to enable the public to better understand events that may concern public interest and ensure their freedom of speech.[56]

In the context of combating (mis) and (dis)information, as clearly stated in Article 12 of the *Provisions*, users' personal IP territoriality is required to be reasonably disclosed "so that the public may supervise for the public interest", which echoes the scenario of "public supervision" in the PIPL Article 13 Paragraph 1(5). Notably, this requirement is distinct from the permissive nature of disclosure in the PIPL and relevant doctrines in the Civil Code. The legality of this provision has been discussed in previous literature, which will be out of the scope of this Note.[57] Nevertheless, as departmental rules, the *Provisions* should not be interpreted as coming into conflict with superior legislations, namely the basic principles of PIPL and the specific boundaries set by PIPL Article 13 Paragraph 1(5), the Civil Code Articles 999, and 1036, in which information processors need to weigh the need of public interest against potential impacts on information subject's rights and interests.[58] In light of this, we argue that platforms still need to justify the choice of disclosing personal information for combating (mis) and (dis)information through PIPL Article 13 Paragraph 1(5) in every single processing activity. Without this process, it is illegitimate to disclose all users' IP territoriality without obtaining their consent.

Two issues would then arise. First, it is worth investigating whether and to what extent disclosing all users' IP territoriality, rather than merely disclosing the information of related parties in specific events, would fall within the scope

[55] *See* Jiang Zhanjun (姜战军), *Minfadian Renge Liyi Heli Shiyong Yiban Tiaokuan Yanjiu* (民法典人格利益合理使用一般条款研究) [*A Study on the General Clause of Fair Use of Personality Interests in the Civil Code*], 3 ZHONGGUO FAXUE (中国法学) [CHINA LEGAL SCI.] 82, 92 (2023).

[56] *See* Zhang Xinbao (张新宝), *Lun Geren Xinxi Baohu Fa Dui Chuanmei Huodong De Shiyong* (论《个人信息保护法》对传媒活动的适用) [*On the Application of the Personal Information Protection Law to Media Activities*], 6 XIANDAI CHUBAN (现代出版) [MODERN PUBLISHING] 46, 47 (2021).

[57] *See* Wang Dongfang (王东方), *Wangluo Pingtai Gongkai Yonghu IP Shudi Xinxi De Shifaxing Fenxi* (网络平台公开用户IP属地信息的适法性分析) [*Analysis of the Lawfulness of the Network Platform to Disclose the User's IP Territorial Information*], 5 XINJIANG SHEHUI KEXUE (新疆社会科学) [SOC. SCI. IN XINJIANG] 123, 128 (2022).

[58] *See* Minfa Dian (民法典) [The Civil Code] (promulgated by the Nat'l People's Cong., May 28, 2020, effective Jan.1, 2021), CLI.1.342411 (Chinalawinfo). According to Article 999, whoever conducts acts as news reporting and supervision by public opinions for public interest may properly use the name, portrait, and personal information. Article 1036(3) also stipulates that an actor will not assume any civil liability if the personal information processing is reasonably conducted to protect the public interest.

of public opinion supervision. The legal basis in the PIPL Article 13(5) is primarily designed to help promote the transparency of information related to public figures or relevant parties in illegal or immoral events so that the public could have access to associated information. Publishing and disseminating (mis) and (dis)information may possibly become illegal when it has a negative impact on public interests and needs public opinion supervision. In particular, users of social media gradually become would-be journalists.[59] Even if some of them have not been related parties in a specific event, they are capable of telling others' stories. Thus, one possible explanation of why Article 12 of the Provisions might fall within the PIPL Article 13 Paragraph 1(5) is that disclosing all users' IP territoriality is aimed at reducing potential risks of disseminating false information and helping other recipients identify reliable sources by comparing the geolocation of publishers with the places of the events in controversial posts or comments.[60] However, as further explained in Part IV, not all users' personal information will be relevant to the objective of combating (mis) and (dis)information. A contextualized analysis needs to be conducted prior to processing activities to ensure that disclosing users' information will be genuinely conducive to the aim of increasing transparency and preventing from spreading (mis) and (dis)information.

Second, even if mandatorily disclosing internet service users' personal information pertains to the public interest, it is essential to enquire how the legal exception of obtaining individual consent could be controlled within a reasonable scope. Different from individual consent, legal bases for processing personal data are provided for striking a balance between the free flow of information in certain circumstances and the need to protect personal rights and interests related to personal information. Nevertheless, as tools for constraining personal rights and interests, these legal bases are not limitless. Processing activities based on Article 13 Paragraph 1(2)-(7) are justified only when they are confined within a necessary and reasonable scope.

Two sources in the PIPL may provide the further specification of the "reasonable scope." From the outset, these crucial thresholds in Article 13 are the specific embodiments of general principles of processing personal information in the PIPL.[61] General principles could also provide further guidance on how to interpret the "reasonable scope." For instance, the "purpose limi-

[59] *See* Briony Swire & Ullrich Ecker, *Misinformation and Its Correction: Cognitive Mechanisms and Recommendations for Mass Communication*, *in* MISINFORMATION AND MASS AUDIENCES 195, 196 (Brian G. Southwell et al. eds., 2021).

[60] *See* Ning Xuanfeng (宁宣凤), Wu Han (吴涵) & Yao Minlv (姚敏侣), *Quanmian Jiedu Huanlianwang Yonghu Zhanghao Xinxi Guanli Guiding* (全面解读《互联网用户账号信息管理规定》) [*A Comprehensive Interpretation of the "Provisions on the Management of Internet User Account Information"*], KING & WOOD MALLESONS (Jul. 1, 2022), https://www.kwm.com/content/kwm/cn/zh/insights/latest-thinking/speech-infidel-line-in-vain-a-comprehensive-interpretation-of-the-internet-user-account-information-management-regulations.html.

[61] *See* Liu Quan (刘权), *Lun Geren Xinxi De Hefa, Zhengdang, Biyao Yuanze* (论个人信息处理的合法、正当、必要原则) [*On the Principle of Legality, Legitimacy, and Necessity in the Personal Information Processing*], 5 FAXUE JIA (法学家) [THE JURIST] 1, 4 (2021).

tation" principle (Article 6 Paragraph 1), the "minimum necessary" principle (Article 6 Paragraphs 1 and 2), and the security principle (Article 9) in the PIPL should all be complied with in all personal information processing activities and could fill the gap in legislative interpretations. Second, the obligation of personal information protection impact assessment in PIPL Article 56 provides for more concrete mechanisms of assessing whether means of personal information processing is proportionate to its aims: "the personal information protection impact assessment should consider three perspectives: (i) whether the purposes and methods of processing of personal information, among others, are lawful, legitimate, and necessary; (ii) the impacts on individuals' rights and interests and security risks; and (iii) whether the protection measures taken are lawful, effective, and suitable to the degree of risk." This obligation of impact assessment is compulsory when personal information is intended to be disclosed (Article 55). These requirements clearly show that the legitimate interests behind processing activities must be weighed against the potential harm to individuals before personal information is disclosed or processed in other methods.

C. Summary

Compared with the PIPL Article 13 Paragraphs (3) and (7), Article 13 Paragraph 1(5) might be more likely to provide a legal basis for online platforms to disclose users' IP territoriality with the aim of reducing (mis) and (dis)information. Both general principles of processing personal information and the regime of personal information protection impact assessment could be explored to enrich the explanation of "reasonable scope" in Article 13 Paragraph 1(5). Following this, it remains to explore how to integrate general principles of processing personal information into different stages of the impact assessment. This significantly matters not only because the *Provisions* Article 12 has granted wider discretion to online platforms to strike the delicate balance between competing rights and interests, but also because online platforms need guidance to help them respond to the dynamic and uncertain nature of social media immediately and responsibly. In Part IV, we will argue that the framework of proportionality could potentially provide a structure to integrate both regimes and accommodate the practical need of information processors to balance using personal information to regulate (mis) and (dis)information against the potential harm and risks to individual rights and interests.

IV. BALANCING PERSONAL INFORMATION PROTECTION WITH COMBATING (MIS) AND (DIS)INFORMATION: AN ANALYSIS OF DISCLOSING USERS' IP TERRITORIALITY

The proportionality principle has long been used for preventing administrative and legislative power from excessively derogating personal rights and interests, but also for multiple checks and balances in private law. This is particularly the case when some private actors could combine extensive powers

in their hands in a way by creating self-regulatory frameworks of norms, quasi-executive, and quasi-judicial functions.[62] For example, when private personal information processors use legal bases other than information subjects' consent, individuals' autonomy over personal information is severely constrained as they have no chance to participate in negotiations with information processors before initiating processing.[63] In this context, the framework of proportionality is a valuable tool to arrive at a rational determination by breaking the complex question of whether the interference with the right or interest is justified into several sub-questions.[64] More specifically, as illustrated below, the idea of proportionality has been embodied in the section of "General Principle" and the specific rule of personal information protection impact assessment in the PIPL, even though it has not been clearly listed as one fundamental principle of processing personal information.[65]

In general, the test of proportionality may entail four sub-tests. First, an explicit, specific, and reasonable purpose would be the prerequisite of conducting proportionality test.[66] The remaining three sub-tests examine the relationship between the means and the ends. They also serve as the foundation for our analytical framework in the upcoming discussions. The second stage "suitability" requires that the means should be directly related to and positively advance the legitimate purpose that is pursued by the personal information processors.[67] The third stage "necessity" starts taking into account the other side of the scale – "impacts on individuals' rights and interests and security risks." Among multiple alternative processing activities that are suitable for achieving the legitimate purpose, the test of necessity obliges the processors to find the way which imposes the least negative restrictions on individuals' personal information. Moving to the final stage – proportionality in the narrow sense, personal information processors will weigh the benefits gained by the processing activities against the interference with the individuals' rights and interests related to personal information, which have already been identified in the first and second stages respectively.[68] This stage further implies that the fulfillment of the proper purpose – even by suitable means that are least restrictive to individuals' rights and interests – cannot lead to a disproportionate limitation of personal information. The heavier an interference with indi-

[62] *See* Enguerrand Marique & Yseult Marique, *Sanctions on Digital Platforms: Balancing Proportionality in a Modern Public Square*, 36 COMPUTER L. & SECURITY REV. 105372, 4 (2020).

[63] *See* Lorenzo Dalla Corte, *On Proportionality in the Data Protection Jurisprudence of the CJEU*, 12 INT'L DATA PRIVACY L. 259, 265 (2022).

[64] *See* K. Moller, *Proportionality: Challenging the Critics*, 10 INT'L J. CONST. L. 709, 727 (2012).

[65] *See* CHENG, *supra* note 30, at 81–82; Liu, *supra* note 61, at 8–12.

[66] *See* Moller, *supra* note 64.

[67] *See* AHARON BARAK, PROPORTIONALITY : CONSTITUTIONAL RIGHTS AND THEIR LIMITATIONS 303 (2012).

[68] *See id.*, at 340.

viduals' rights and interests, the greater the importance of satisfying the other pressing social needs.[69]

As regards the first sub-test, the PIPL Article 6 stipulates that the purposes of disclosing personal information should be specific, explicit, and reasonable. This provision echoes the requirement of proper purposes in the proportionality test. As mentioned in the introduction, the disclosure of users' IP territoriality is intended to prevent users from pretending to be related parties in high-stake events or fabricating disinformation.[70] Therefore, combating (mis) and (dis)-information would be the purpose for the disclosure of users' personal information. This purpose could be seen as related to public interest as fake news can impose great threats to democracy and fuel social panic during crises. Social media platforms further increased their influence with greater spreading speed and volume.[71] That is also the reason that the *Cybersecurity Law* Article 47 and the *Regulation on Internet Information Service* Article 15(6) require internet information service providers to prevent the dissemination of (mis) and (dis)information once they found the information may disturb social order or stability.

That said, it should be noted that the purpose chosen by the information processors is legitimate and proper does not necessarily mean that the processing activity is proportionate. After finding the proper purpose, we will further examine the relationship between the means and the ends and see how the suitability, necessity, and proportionality in the narrow sense will enrich the analysis of "reasonable scope" in the PIPL Article 13 Paragraph 1(5). The following discussion does not intend to provide a one-size-fits-all answer to when the disclosure of users' personal information is absolutely proportionate. This is because the delicate balance needs to be struck in each individual case by paying attention to the complexity of the specific contexts, which may include but are not restricted to the nature of social media users' speech, the scale of disclosing personal information, the scale of (mis) and (dis)information dissemination and so forth.

A. Suitability

The test of suitability requires that the means of constraining personal information is directly related to and can advance the purpose that is pursued

[69] *See* Robert Alexy, *Proportionality and Rationality*, *in* PROPORTIONALITY: NEW FRONTIERS, NEW CHALLENGES 13, 16 (Vicki C. Jackson & Mark Tushnet eds., 2017).

[70] *See* Weibo Administrator, *supra* note 13.

[71] Vosoughi *et al.* found that false news stories "diffused significantly farther, faster, deeper, and more broadly than the truth in all categories of information." *See* Soroush Vosoughi, Deb Roy & Sinan Aral, *The Spread of True and False News Online*, 359 SCIENCE 1146, 1146 (2018). They investigated approximately 126,000 news stories on Twitter between 2006 and 2017. Using data from six independent fact-checking organizations, the researchers classified the news stories into true and false, and compared their influence. *See also* Gautam Kishore Shahi, Anne Dirkson & Tim A. Majchrzak, *An Exploratory Study of COVID-19 Misinformation on Twitter*, 22 ONLINE SOCIAL NETWORKS AND MEDIA 1, 1 (2021).

by the personal information processors.[72] Though PIPL Article 6 does not use the word "suitability," it states that processing personal information should be "directly related to those purposes." This direct relation should be interpreted as the processing activities could positively increase rather than negatively hinder the realization of the stated purpose. If processing personal information may further exacerbate the risks of being exposed to (mis) and (dis)information, it may not be able to positively advance the stated purpose.

In the context of countering (mis) and (dis)information in social media, therefore, the core issue of suitability is whether the specific method of disclosure is "directly related to" and can further advance the claimed purpose.

In the era of social media, users with more information literacy to navigate and locate information in the digital world are assumed to be more likely to identify (mis) and (dis)information.[73] Nevertheless, critical-thinking skills and having knowledge about the news-making processes may not be enough to discern reality from fabricated stories, as distorted stories could resemble the format and content of real stories.[74] Even though users could have the ability and willingness to voluntarily search for relevant information to verify controversial messages, it is still challenging to effectively pinpoint the truth from a tremendous range of disorganized digital sources. It is in this sense disclosing certain users' IP territoriality might be related to the aim of providing more resources for fact-checking, as this countermeasure is likely to help the recipients to formulate their own judgments when a news story distorts details about geolocations. For instance, a Beijing social media user may release a detailed article and allege that it happened a moment ago in Shanghai. Readers naturally will doubt if the author has verified all the details due to the long distance. Although the news story may not necessarily be (mis) and (dis)information, the audience's caution is a "first line of defense" against information manipulation.[75] Another example would be that, since Xiaohongshu revealed the IP territoriality of all bloggers, users could identify "fake agents" who live in China but pretend to share their everyday lives in other countries and advertise products.[76]

Nevertheless, the above discussion may merely reveal the relationship between disclosing users' IP territoriality and countering (mis) and (dis)information on an abstract level. The assessment of suitability should surround

[72] *See* BARAK, *supra* note 67, at 303.

[73] *See* Hendrik Heuer & Andreas Breiter, *Trust in News on Social Media*, PROCEEDINGS OF THE 10TH NORDIC CONFERENCE ON HUMAN-COMPUTER INTERACTION 137, 137 (2018). This research finds that German high school students could make meaningful trust ratings that differentiate quality and fake news, and their trust ratings correspond to expert rankings of the news sources.

[74] *See* S. Mo Jones-Jang, Tara Mortensen & Jingjing Liu, *Does Media Literacy Help Identification of Fake News? Information Literacy Helps, but Other Literacies Don't*, 65 AM. BEHAVIORAL SCIENTIST 371 (2019).

[75] *See* Maria Glenski et al., *User Engagement with Digital Deception*, *in* DISINFORMATION, MISINFORMATION, AND FAKE NEWS IN SOCIAL MEDIA: EMERGING RESEARCH CHALLENGES AND OPPORTUNITIES 39, 41 (Kai Shu et al. eds., 2020).

[76] See *IP Shudi Gongneng Yinfa Reyi* (IP属地功能引发热议) [*The Function of IP Territoriality Has Sparked Heated Discussions*], SOHU (May 9, 2022), https://www.sohu.com/a/545310728_121066095.

the nature of specific processing activities. The way of disclosing users' personal information in social media for countering (mis) and (dis)information is anticipatory, persistent, compulsory, and on a large scale. These features set the disclosure of users' IP territoriality different from the more pervasive method of disclosing certain individuals' personal information in a single news event. Following this, the test of suitability needs to put more emphasis on whether these features are all directly related to and could alleviate (mis) and (dis)information. There are at least three caveats that need to be taken into account when examining the suitability of disclosing users' IP territoriality.

1. Are All Posts and Comments Related to Public Opinion Supervision? To start with, it is questionable that all posts and comments on social media need to be supervised by public opinion. The fair use of personal information for the purpose of public opinion supervision primarily intends to help promote the transparency of information related to public figures or relevant parties in illegal or immoral events so that the public could have access to associated information to ensure their freedom of speech.[77] The *Criminal Law* Article 291 (I), the *Public Security Administration Punishments Law* (治安管理处罚法)[78] Article 25, and the *Regulation on Internet Information Service* Article 15 all require the illegal (mis) or (dis)information to be verifiably inaccurate information which has the impact of "disturbing social order and stability." Only when these conditions are satisfied can individuals who publish or knowingly spread (mis) and (dis)information fall within the scope of public opinion supervision. However, a tremendous number of posts and comments on social media could be personal opinions that cannot be verified as true or false. Also, countless posts or comments are completely about the individual's daily life without harming the public order.

2. Are All Posts and Comments Related to (Mis) and (Dis)Information Connected to Geolocation? Second, the (mis) and (dis)information producing process is variable and complex. In many cases, if the factual statement awaiting confirmation is not related to one's location, it may be difficult for the disclosure of IP territoriality to prove its relevance for fact-checking purposes.

For instance, around May 11, 2022, a Shanghai resident shared in a Wechat group a video that showed three people wearing protective coveralls breaking into a typical Shanghai apartment. Alongside the video, a photo of a broken door was displayed.[79] The publisher alleged that the three people were health

[77] *See* Jiang, *supra* note 55, at 92.

78 Zhi'an Guanli Chufa Fa (治安管理处罚法) [Public Security Administration Punishments Law] (promulgated by the Standing Comm. Nat'l People's Cong., Aug. 28, 2005, rev'd Oct. 26, 2012), CLI.1.188539 (Chinalawinfo).

[79] See *Louli Yinxing Bei Lazou, Meijiao Yaoshi Bei Qiaomen?* (楼里阴性被拉走，没交钥匙被撬门?) [COVID-Free Residents Were Dragged Away and Their Homes Were Broken Into?], SHANGHAI WANGLUO PIYAO (上海网络辟谣) [SHANGHAI CYBERSPACE RUMOR REFUTATION] (May 11, 2022), https://mp.weixin.qq.com/s/shVM671ih-dA5ezbPNmNDw (last visited Jul. 27, 2022).

care givers, and that they were breaking in to sterilize the apartment. The message was further disseminated to other platforms and finally turned out to be disinformation. In fact, the video and the photo are from different sources. The three people in the video were policemen, and they were breaking in to arrest a criminal. That is why one of the three individuals was videotaping the breaking-in process as a law enforcement record.[80] Meanwhile, some other person took a photo of the broken door when his neighbour went home without the key and requested firefighters to pick the lock. The video and the photo were deliberately merged by someone to shape the perception that the neighbour's home was unlawfully entered and sterilized without permission.[81] Before public authorities had time to refute the disinformation, many users had believed and shared it, causing much fear across multiple social media platforms (e.g., Weibo) that healthcare professionals would break in Shanghai citizens' homes only to sterilize. In this event, the location of the publisher did correspond to where the photo was actually taken not only at the level of provinces but also in the specific neighborhood. Nevertheless, the original publisher's location did not seem to help the audience identify (mis) and (dis)information, as it is not the location, but rather the identity of people who broke in and the exact reason that trigger confusion and fear among the audience and awaits further clarification.

This example further indicates one potential limitation of anticipatory disclosure. The content of each piece of (mis) and (dis)information can vary case by case, which implies that it is difficult to predict which specific details should always be disclosed *ex ante* so that the recipients on social media could be more prudent when forwarding the post and comment in question.

3. Will Disclosing Users' IP Territoriality Always Improve Users' Judgment over Controversial Information? Third, it is worth noting that the interaction between disclosing personal information and users' elaboration that may be conducive to weakening the spread of (mis) and (dis)information. The social media environment has not only blurred the line between news producers and consumers but also create more opportunities for individuals to participate in the process of fact-checking. As suggested in one research, there are more replies and quotes among fact-checking tweets (> 20%) than tweets of misinformation (10%), indicating that fact-checking is a more conversational task.[82] Elaboration provides additional details regarding a particular news

[80] See *Shanghai You "Dabai" Qiangxing Pomenerru? Yuanlai Shi Jingcha Zhuabu Fanzui Xianyiren* (上海有"大白"强行破门而入? 原来是警察抓捕犯罪嫌疑人) [*"Big White" in Shanghai Broke into Residents' Homes? It Was the Policemen That Were Arresting Criminal Suspects*], SHANGHAI WANGLUO PIYAO (上海网络辟谣) [SHANGHAI CYBERSPACE RUMOR REFUTATION] (May 11, 2022), https://mp.weixin.qq.com/s/Rz_w6dr_khZZh_P2LVst4w (last visited Jul. 27, 2022).

[81] *See supra* note 79.

[82] *See* Chengcheng Shao et al., *Hoaxy: A Platform for Tracking Online Misinformation*, *in* PROCEEDINGS OF THE 25TH INTERNATIONAL CONFERENCE COMPANION ON WORLD WIDE WEB - WWW '16 COMPANION 745, 748 (2016), http://dl.acm.org/citation.cfm?doid=2872518.2890098 (last visited Jun 3, 2023).

story. Users of social media tend to counterbalance their limited engagement by relying on other users' commentary about the news story's credibility.[83] Therefore, when more comments offer additional information, the recipients may think more deeply instead of simply believing the news story. Moreover, herd mentality[84] means a higher rate of elaboration is possible to encourage other users to also make more elaboration in their comments, resulting in a richer information environment for the audience to make judgment calls on the reliability of news stories. Hence, a policy that incentivizes users to post elaborations has the potential to help weaken the originally great influence of (mis) and (dis)information.

If disclosing more users' personal information can promote elaborations in users' reactions, it is a good sign that the disclosure may work in fighting fake news. However, it is unclear whether disclosing more personal information can encourage users to elaborate on their comments. For instance, Disqus, an online blogging platform, allows users to make comments under real names, anonymity, or pseudonyms. Data on Disqus in 2012 showed that pseudonym users posted more comments and generated richer discussions than users of real names.[85] Even though this research does not disclose personal geolocation, it suggests that disclosing more users' personal information is not necessarily effective in promoting elaboration to counter (mis) and (dis)information. Promoting public opinion supervision and countering (mis) and (dis)information is premised on encouraging social media users' freedom of speech.[86] Disclosing social media users' IP territoriality thus could be a double-edged sword. The freedom of expression not only requires the free flow of information that can enable users to make comprehensive judgments but also provides safeguards to protect users' personal information when they engage in public opinion supervision. When assessing the suitability of disclosing users' IP territoriality, therefore, online platforms should also take into account the potential chilling effect on users' engagement in fact-checking and commenting on controversial posts.

4. Summary. The above caveats intend to illustrate the uncertainties with disclosing users' IP territoriality anticipatorily and on a large scale in order to counter (mis) and (dis)information. The test of suitability does not require the measure in question to be the only way of realizing the alleged legitimate

[83] *See id.*

[84] Herd mentality refers to "the tendency of the people in a group to think and behave in ways that conform with others in the group rather than as individuals." See *Herd Mentality*, MERIAM-WEBSTER DICTIONARY, https://www.merriam-webster.com/dictionary/herd%20mentality (last visited Jul. 27, 2022).

[85] *See* Erick Schonfeld, *61 Percent Of Disqus Comments Are Made With Pseudonyms*, TECHCRUNCH (Jan. 10, 2012), https://techcrunch.com/2012/01/09/61-percent-disqus-comments-pseudonyms/ (last visited Jun 3, 2023).

[86] *See* Zhang Xinbao (张新宝), *Yanlun Biaoshu He Xinwen Chuban Ziyou Yu Yinsiquan Baohu* (言论表述和新闻出版自由与隐私权保护) [*Freedom of Speech, Freedom of the Press, and Privacy Protection*], 6 FAXUE YANJIU (法学研究) [CHINESE JOURNAL OF LAW] 32, 34–35 (1996).

purpose. In general, the means in question could fit the ends if it could sufficiently advance the purpose.[87] However, it should be noted that the relationship between the standard of review and the level of interference with rights and freedoms. The greater the intensity of the interference, the more information is essential to prove its suitability to achieve the pressing social needs pursued by the measure in question.[88] The suitability test is a degree, rather than a threshold test.[89] This test might be useful particularly after the *Provisions* grant a wide discretion to social media platforms. If social media platforms determine to disclose IP territoriality on a large scale, for an extended time period, or in a more precise method, they have to prove that previous solutions may not be sufficient to redress the issue and more evidence is essential to prove the suitability of the measure to respond to the questions we have proposed.

B. Necessity

The test of necessity would further take into account the other end of the scale and evaluate the potential impact on the information subjects from the policy in question. The test of necessity intends to choose which means would have the least interference with the rights and freedoms of people who will be affected by the means.[90] This requirement is clearly stated in PIPL Articles 5 and 6. According to Article 6, the specific meaning of necessity in the PIPL refers to "minimum necessary". Personal information should be processed "in a manner that has the minimum impact on rights and interests of individuals" (Article 6 Paragraph 1) and "collection of personal information shall be limited to the minimum scope necessary for achieving the processing purpose and shall not be excessive" (Article 6 Paragraph 2).

More specifically, the PIPL Article 56(1) and (2) could be deemed as two fundamental elements of the necessity test. As the test of necessity aims at controlling the intrusiveness to people's rights and freedoms to the least level, the assessment of necessity in Article 56(1) is premised on the evaluation of the impact on individual rights and security risks in Article 56(2).

1. Identify the Potential Impact on Users' Rights and Freedoms. In order to elaborate the framework of evaluating impacts on information subjects, we incorporate factors considered under the PIPL Article 51 and the *Information Security Technology – Guidance for Personal Information Security Impact Assessment* ("*Guidance for PISIA*") to provide a non-exhaustive checklist for potential information processors.[91] These factors all manifest a contextual

[87] *See* BARAK, *supra* note 67, at 305–306.

[88] *See* JONAS CHRISTOFFERSEN, FAIR BALANCE: PROPORTIONALITY, SUBSIDIARITY AND PRIMARITY IN THE EUROPEAN CONVENTION ON HUMAN RIGHTS 187 (2009).

[89] *See id.*

[90] *See* BARAK, *supra* note 67, at 317.

[91] As suggested in the PIPL Article 51, processors should take into account "the purposes, methods of processing personal information, the nature of personal information, the impacts on individuals' rights and interests, and potential security risks" when selecting technical measures to ensure personal information

consideration of assessing the risks and selecting what countermeasures should be conducted. They will be integrated into four perspectives in this Note and illustrated against the background of disclosing social media users' personal information to combat (mis) and (dis)information as below.

a. Methods of Processing Personal Information and Third Parties' Actions. In light of the methods of processing personal information, online platforms ought to take into account the amount of personal information; for how long; how many people could have access to the personal information; whether the personal information is processed or combined with other data; and whether the processing concerns profiling of individuals or the usage of automated decision-making system. When disclosing social media users' information to combat (mis) and (dis)information, it is also critical for online platforms to consider the scope of disclosure and third parties' potential actions after having access to the processed personal information.

According to some social media platforms' information policies, every user is mandated to disclose their IP territoriality to the public so that the IP territoriality can be accessed by anyone unless users set restrictions by themselves.[92] The number of monthly active users for multiple social media platforms in China has exceeded 100 million.[93] Before modifying information policies, every user's IP territoriality will renew every time people post or comment and be displayed permanently.

Normally, unlimited access to users' personal information may possibly lead to stalking, harassment, domestic violence, identity theft, or fraud.[94] These risks are highlighted when Facebook's real name policy made some victims of stalking and domestic violence more vulnerable.[95] People in the LGBTQ group may face harassment offline after disclosing their real names on social

security. In addition, according to the *Guidance for PISIA* Paragraph 4.6, the scope of personal information security assessment is conditioned on the nature of affected personal information, the status of personal information subjects, and who could have access to personal information.

[92] *See e.g.*, Weibo Administrator, *supra* note 13; *Xiaohongshu Yonghu Yinsi Zhengce* (小红书用户隐私政策) [*Privacy Policy for users of Xiao Hong Shu*], XIAO HONG SHU (小红书) (2023), http://www.xiaohongshu.com/mobile/privacy (last visited Jun 3, 2023).

[93] See *2023 Nian Shejiao Pingtai Yanjiu Baogao* (2023年社交平台研究报告) [*Research Report on Social Media Platforms in 2023*], 21 JINGJI WANG (21经济网) (Apr. 6, 2023), https://www.21jingji.com/article/20230406/herald/f0abad82d28575aa291da27df055ccbb.html (last visited Jun 3, 2023).

[94] *See* Cassie Cox, *Protecting Victims of Cyberstalking, Cyber Harassment, and Online Impersonation Through Prosecutions and Effective Laws*, 54 JURIMETRICS 277, 278 (2014). This research illustrates cyberstalking with an example where a woman was threatened with rape because her personal information was posted by others as an advertisement about fantasies of being raped. *See also* Danielle Citron, *Mainstreaming Privacy Torts*, 98 CALIF. L. REV. 1805, 1817–18 (2010). This research discusses a similar example that someone posted "a teenager's picture, work address, cell phone number, and email address" suggesting her rape fantasies, causing her to be confronted by men after work.

[95] *See* Samantha Allen, *How Facebook Exposes Domestic Violence Survivors*, DAILY BEAST (Apr. 14, 2017), https://www.thedailybeast.com/how-facebook-exposes-domestic-violence-survivors (last visited Jul. 27, 2022).

media.[96] To prevent this risk, they may choose to hide their identity on social media, losing an essential way to connect with others in the community. Although the likelihood of such risks may not be great, the consequence can be extremely serious. At present, the level of geolocation shown through IP territoriality is nations or provinces. It might be difficult for people to precisely locate the user without other information. However, since IP territoriality has been disclosed, some users of Weibo have faced online fraud. Some would copy profile photos and nicknames of individual users to scam followers of these users. By showing the same IP territoriality, scammers may further increase the credibility of these imitating accounts and impose more risks on users' and followers' property security.[97]

It is also relevant to consider whether disclosing more personal information on social media may also increase targeted (mis) and (dis)information.[98] This aspect is also related to the test of suitability to some extent. Many suggested contents are targeted to users by analyzing their political beliefs, age, locations, and gender.[99] Under PIPL Article 13(6), any third party is allowed to reasonably process personal information that has been legally disclosed. After social media platforms mandate the disclosure of certain personal information, publishers of (mis) and (dis)information would be able to micro-target audiences to whom (mis) and (dis)information will have the greatest impact according to their IP territoriality. Moreover, since the disclosure is mandated instead of obtaining information subjects' consent, users may suffer risks of receiving unwanted automatic recommendations unless platforms provide opportunities to opt out.[100] The risk of targeted (mis) and (dis)information has both a high likelihood to materialize and a serious consequence.

b. The Status of Information Processors and Information Subjects. The status of information processors matters because richer resources generally lead to greater negotiating power against individual information subjects. Article 12 of the *Provisions* gives platforms discretion to decide the "reasonable" scope of users' IP territoriality that should be mandatorily disclosed. On one hand, this rule is more flexible to adapt to different circumstances of balancing personal information against the public interest. On the other hand, however, this provision may further increase platforms' power to decide when they

[96] *See* Jillian C York & Dia Kayyali, *Facebook's "Real Name" Policy Can Cause Real-World Harm for the LGBTQ Community*, EFF (Sep. 16, 2014), https://www.eff.org/zh-hans/deeplinks/2014/09/facebooks-real-name-policy-can-cause-real-world-harm-lgbtq-community (last visited Jul. 27, 2022).

[97] See *Tixing Gewei Zai Haiwai De Xiao Huoban Xiaoxin Weibo Zhapian* (提醒各位在海外的小伙伴小心微博诈骗) [A Reminder to All Buddies Overseas to Beware of Scams on Weibo] (Jul.3, 2022) https://weibo.com/6660835434/Laz2n8Uub?filter=hot&root_comment_id=4787158865156407&ssl_rnd=1658506625.2625&type=comment (last visited Jul. 27, 2022).

[98] *See* Unger, *supra* note 21, at 324–27.

[99] *See* Alex Campbell, *How Data Privacy Laws Can Fight Fake News*, JUST SECURITY (Aug. 15, 2019), https://www.justsecurity.org/65795/how-data-privacy-laws-can-fight-fake-news/ (last visited Jul. 27, 2022).

[100] *See id.*

assume it is necessary to disclose specific personal information of all users. If the information processor has a dominant position in the market, users will likely have limited alternatives if they want to opt out of its policy on personal information.[101] This is especially true for social media due to their network effects. Even if a user of Wechat and Weibo does not like the specific policies, he/she can hardly switch to another social platform because most of his/her friends use Wechat and Weibo. Hence, users may reasonably expect greater protection to personal information from market-leading controllers.[102]

The vulnerability of information subjects needs also to be considered. As per the PIPL Article 28, information of minors under the age of fourteen has already been protected as sensitive information that could easily lead to the violation of the personal dignity of a natural person or harm to personal or property safety. Other groups belonging to a more vulnerable segment of the population, such as the mentally ill, the elderly, the LGBTQ groups, etc., may need special protection as well. It should be considered if the disclosure of IP territoriality will impose any specific negative impact on their rights and freedoms.

c. The Nature of Processed Personal Information. The nature of the disclosed information may be relevant. Article 12 of the *Provisions* does not provide how precisely users' IP territoriality should be disclosed. According to the current practice, IP territoriality is limited to users' nations or provinces, which will not normally constitute personal whereabouts that are categorized as "sensitive information" in the PIPL Article 28. Personal whereabouts in the PIPL include both the precise real-time geographical location of individuals at a specific time, and the information that people travel from one place to another, such as train ticket information.[103] However, it should be noticed that platforms could determine what level of personal geolocation might be reasonable to disclose. That said, the more details one's IP territoriality involves, the more

[101] *See* Article 29 Data Protection Working Party, *Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller Under Article 7 of Directive 95/46/EC*, 43 (2014).

[102] In fact, U.S. users have protested against Facebook's real name policy, *see e.g.*, https://www.aclunc.org/sites/default/files/20151005-fb_open_letter.pdf (last visited Jul. 27, 2022). Also, before the *Provisions* have been officially passed, a Chinese user, a student from Zhejiang Sci-Tech University, sued Weibo for forcing users to disclose their IP territoriality. Relevant news could be seen in Li Yu (李宇), *IP Dizhi Xinxi Gongkai Suoshe Hegui Wenti Fenxi* (IP地址信息公开所涉合规问题分析) [*Analysis of Compliance Issues Involved in Disclosure of IP Address Information*], JIN CHENG TONG DA (金诚同达) [JT&N] (May 16, 2022), https://mp.weixin.qq.com/s/8dvMpvvDdiaDxaD3aXjyKQ (last visited Jul. 27, 2022). Other opposing views could be seen in *Bo Zhichi Gongkai IP Shudi de Jiutiao Miulun* (驳支持公开IP属地的九条谬论) [*Refuting Nine fallacies in Favor of Public IP Territoriality*], ZHIHU (May 3, 2022) https://zhuanlan.zhihu.com/p/508234267 (last visited Jul. 27, 2022).

[103] *See* Zhang Liang (张梁), *Danci Goupiao Nenggou Wanzheng Fanying Xingzong Guiji Xinxi* (单次购票能够完整反映行踪轨迹信息) [*A Single Ticket Can Fully Reflect the Personal Whereabouts Information*], JIANCHA RIBAO (检察日报) [PROCURATORATE DAILY] (Sep. 25, 2017), https://www.spp.gov.cn/llyj/201709/t20170925_201401.shtml (last visited Apr 20, 2023).

sensitive the disclosed IP territoriality would be and the more risks relevant to users' personal security should be taken into account.

d. The Affected Rights and Freedoms. The harmful effect caused by processing personal information is not restricted to the limitation to individual autonomy to process own information and the invasion of one's privacy but may also be inextricably linked to interference with other types of personal or proprietary rights. Given the increasing imbalance in informational power, the rights and interests of information subjects should be interpreted broadly to protect individuals' autonomy,[104] not only including harms to individual personal or property rights, but also including group harms like discrimination, and social harms, such as chilling effect on public debates.[105]

As mentioned in the previous section, when social media platforms determine whether and the scope of disclosing users' personal information, it is worth considering how likely the disclosure may cause adverse emotional impacts and have chilling effects on public debates. For example, after Weibo mandated users to disclose IP territorialities, some users suffered cyberbullying merely because of where they were staying.[106] Discrimination associated with geographical locations may disturb peaceful orders on social media and create chilling effects on public discussions, as users may fear that others would focus on their IP territorialities more than the content of their speech.[107] This may discourage, rather than promote public opinion supervision of public figures or those who participate in high-stake social events, which is the original aim of Article 13 Paragraph 1(5) PIPL. Also, as discussed above, the compulsory disclosure of IP territoriality, particularly when combined with other voluntarily posted information, may pose a risk of being physically stalked or harassed to vulnerable groups. Such a strategy can restrict users' ability to use social media for more than just receiving information, but also serving as a means for telling their own stories or advocating for their rights.

2. Find the Least Intrusive Means. After identifying different alternatives' potential impact on people's rights and freedoms, the data processors need to further find the measure which will restrict personal rights and freedoms at the least level. The specific intensity of review in this stage could also be seen in the PIPL Article 6. Applied in personal information protection, a processing activity is permitted only when it is "limited to the

[104] *See* CHENG, *supra* note 30, at 430; Article 29 Data Protection Working Party, *supra* note 101, at 30.

[105] *See id.*

[106] Some comments on discrimination could be seen at https://weibo.com/7313424863/Lu3y8shRO?type=comment#_rnd1658188285765 (last visited Jul. 27, 2022), and https://weibo.com/1263406744/LwrsFfraP?refer_flag=1001030103_&type=comment#_rnd1658188398877 (last visited Jul. 27, 2022).

[107] See *IP Shudi Gongkai Yinian Hou* (IP属地公开一年后) [*One Year After IP Territoriality Being Displayed*], SOHU (搜狐) (May 20, 2023), https://www.sohu.com/a/677337389_439656 (last visited Jun 3, 2023).

minimum scope required by the purpose" and "exert[s] the minimum impacts on the rights and interests of individuals."

Compared with disclosing users' IP territoriality in all circumstances, there are at least three less intrusive ways that may achieve the goal of combating (mis) and (dis)information. First, social media users could complain that specific posts or comments as inaccurate information. For example, Weibo will give blue tags for any posts or comments that are disputed to give a warning to any user before they further spread it. If a piece of information is confirmed as (mis) or (dis)information, Weibo will reserve the original post or comment in question and attach a yellow tag which indicates how this piece is different from the truth.[108]

Second, as Chun Peng suggested, platforms could promote the users' judgment of news credibility by allowing users to choose whether they want to disclose IP territoriality.[109] If they select to disclose their IP territoriality, the social media platforms could display their geolocation on the level of countries and provinces according to the IP addresses assigned by the Internet Service Providers rather than freely selected by users. In this way, the audience can consider voluntary disclosure of IP territoriality as enhancing promoter's confidence in news credibility while preserving promoters' autonomy over their personal information.

Third, platforms can put more emphasis on financially interested entities and persons, since they are more motivated than normal users to spread fabricated or twisted news stories to their interest. For instance, Douyin, a leading short video platform, has mandated its users to disclose their Multi-Channel Network ("MCN") partners so that the audience can evaluate if the messages they convey are self-interested.[110]

Though these alternatives may not be able to redress all the needs for tackling (mis) and (dis)information, they could counter the excessive negative impact caused by the conflict between maintaining public interest and the protection of personal information.

3. Summary. To conclude, the test of necessity examines how disclosing social media users' personal information may influence their rights and freedoms. The assessment is premised on how precise the IP territoriality

[108] *See* Weibo Guanliyuan (微博管理员) [Weibo Administrator], *Weibo Shequ Gonggao* (微博社区公告) [*Weibo Community Announcement*] (Jan. 13, 2022), https://weibo.com/1934183965/LayNw8of7?filter=hot&root_comment_id=0&type=comment#_rnd1660824288086.

[109] *See* Peng Chun (彭錞), *IP Shudi Gongkai: Ruhe Pingheng Geren Yinsi Yu Wangluo Zhixu* (IP属地信息公开: 如何平衡个人隐私与网络秩序) [*Disclosing IP Territoriality: How to Balance Personal Privacy and Order in Cyberspace*] (Jun. 29, 2022), https://mp.weixin.qq.com/s/Jh8a8DSeO3FvKiPy6qR-IQ (last visited Jun 3, 2023).

[110] *See* Douyin Zhanghao Xianshi Suoshu MCN Jigou, *Bufen Zhanghao Kaishi "Diaopi"* (抖音帐号显示所属MCN机构，部分帐号开始"掉皮") [*After Douyin Mandates Its Users to Disclose MCN Partners, Some Accounts Start to Lose Credibility*], WANGYI XINWEN (网易新闻) [WANGYI NEWS] (Jul. 22, 2022), https://c.m.163.com/news/a/HCTFE00D0517FQIE.html.

is, how long it is disclosed, the status of information processors and information subjects, and how rights and freedoms are affected.

C. Proportionality in the Narrow Sense

1. Scope of Comparisons. After the sub-tests of suitability and necessity, the benefits and risks of disclosing personal information on social media for the purposes of combating (mis) and (dis)information will be comprehensively assessed in the final step of the proportionality test: proportionality in the narrow sense, which could also be called as the test of balancing.[111] This step aims to examine whether the benefits deriving from the adoption of the measure at issue surpass the potential harms caused by the interference with the protection of rights or interests.[112]

This abstract comparison can be further delineated into two steps – the absolute comparison and the relative comparison. On the absolute level, social media platforms could directly compare the benefits gained by the measure at issue and the harm caused by it. The comparison is not only conducted abstractly between how important the legitimate purpose and the interfered rights or interests are. The comparison should also be conducted between the marginal benefits – the disparity between the state of how the legitimate purpose is fulfilled prior to the measure at issue and the state afterwards, and the marginal harms – the disparity between the state of the interfered rights or interests prior to the measure at issue and the state of affairs afterwards.[113]

On the relative level, social media platforms should further compare the state of affairs after hypothetically implementing alternatives and the state of affairs after the issuance of the measure at issue. Even though some alternatives may not necessarily fulfill legitimate purposes in the same way, they could still be compared with in the last stage of balancing. The measure at issue would be disproportional where an alternative can lead to more reduction of harms to the protected right or interest while resulting in less reduction of the benefits.[114] On the relative level, consequently, online platforms weigh the disparity between the benefits gained by the measure at issue and alternatives against the disparity between the reduction of harms achieved by the measure at issue and alter-natives.[115]

This two-prong approach does not intend to bypass the value-laden comparison between the rights and interests involved. Instead, narrowing down the comparison by focusing on the changes brought up by the issuance of the measure under scrutiny and relevant alternatives could make the determination of the balance more effective.

---

[111] *See* BARAK, *supra* note 67, at 340.
[112] *See* Dalla Corte, *supra* note 63, at 262.
[113] *See* BARAK, *supra* note 67, at 350–51.
[114] *See id.*, at 354.
[115] *See id.*

2. Additional Safeguards After Identifying Disproportionate Measures. Through the careful comparison as illustrated above, platforms need to constantly rework the measure under scrutiny if it is deemed disproportional. As precedingly discussed, alternatives with less harm to personal information should be integrated into the corrective options. In particular, given the dynamic nature of social media, platforms ought to regularly reassess the proportionality of the proposed measures. Platforms should carefully determine the duration, scope, and recipients of IP territoriality at the least intrusive level.

Once determining which measure of disclosing users' personal information is going to be used, additional safeguards could also be taken into account to reduce potential harm to personal information protection and enhance trust between social media platforms and users. Notably but not exclusively, there are several aspects that could be considered.

a. Empowering Information Subjects' Rights. Generally, when personal information is disclosed due to legal exceptions (based on PIPL Article 13 Paragraphs 1(2) to 1(7)), personal choices and autonomy over their information have already been limited, because information processors are not obliged to obtain consent for processing disclosure personal information within a reasonable scope (PIPL Articles 13 and 27).[116] This relaxed scope of protection further alarms the need to examine safeguards to prevent users' personal information from being misused. This is because users may only have limited ability to prevent potential harms that may be caused by subsequent processing activities.[117]

That being the case, platforms could proactively help empower information subjects' rights to opt out of the re-use of disclosed personal information if the only purpose for disclosure is public interest. In the drafts of the first and second readings of PIPL, disclosed personal information was prohibited from being subsequently processed for purposes other than that of disclosure. Though not mandatorily established in the final draft, this requirement provides a caveat for entities who decide to disclose personal information, especially where the balance is difficult to strike. Platforms should be fully equipped with technical and organizational measures to prevent disclosed personal information from being used for purposes other than combating (mis) and (dis)information. For

[116] The law lifts strict criteria upon disclosed information to reconcile the free flow of information and personal interest protection, because it would incur unnecessary burdens for any third party other than the initial processor to identify whether the disclosure is legitimate or not. *See* Liu Xiaochun (刘晓春), *Yi Gongkai Geren Xinxi Baohu He Liyong De Guize Jiangou* (已公开个人信息保护和利用的规则建构) [*Formulating the Rules for the Protection and Utilization of Publicly Disclosed Personal Information*], 2 HUANQIU FALÜ PINGLUN (环球法律评论) [GLOBAL L. REV.] 52, 58–59 (2022).

[117] *See* Cheng Xiao (程啸), *Lun Gongkai De Geren Xinxi Chuli De Falü Guizhi* (论公开的个人信息处理的法律规制) [*On the Legal Regulation of the Processing of Publicly Available Personal Information*], 3 ZHONGGUO FAXUE (中国法学) [CHINA LEGAL SCIENCE] 82, 91–92 (2022); Zhou Guangquan (周光权), *Qinfan Gongmin Geren Xinxi Zui De Xingwei Duixiang* (侵犯公民个人信息罪的行为对象) [*The Object of the Crime of Infringement of Citizens' Personal Information*], 3 QINGHUA FAXUE (清华法学) [TSINGHUA UNIV. L. J.] 25, 35–37 (2021).

example, platforms could provide users with more choices to determine the visibility of their account page and posts. The potential negative impact might be reduced if users could choose to switch off the visibility of their account pages to any third parties on search engines who have not logged on the specific social media platforms. Platforms could also use contractual obligations to limit third parties' reuse of these pieces of disclosed personal information. If so, it may provide further evidence on how to control the negative impact on information subjects. In addition, processors should adopt proper measures of functional separation to enhance the protection of other direct identifiers controlled by processors (e.g., real names, personal ID, telephone numbers, etc.) and prevent disclosed personal information that is indirectly identifiable to be used for re-identification. Otherwise, the lack of safeguards may render users very vulnerable to unexpected negative impacts, which may not justify the assertion that public interest outweighs information subjects' rights and interests.

b. Enhancing Individual Complaint Procedures. According to the PIPL Article 50, processors should establish convenient procedures to recognize and respond to individuals' applications for exercising their rights. These rights, which are stipulated in Chapter IV, are crucial when processors have not disclosed users' personal information within a reasonable scope.[118] For example, users could request processors to delete personal information when the processors violate any law, administrative regulation, or agreement (PIPL Article 47). In the context of combating (mis) and (dis)information, particularly after the *Provisions* become effective, processors may establish unified guidance on the method and scale of disclosure for all users. However, such unified guidance may not ensure specific assessment of individuals when they face unreasonable processing or excessive risks. Therefore, enhancing individual complaining procedures regarding the reasonableness of disclosing personal information is essential to ameliorate potential negative impacts on users.

c. Increasing Transparency. The duty of impact assessment and documentation is based on the accountability principle of information processors which requires a careful test taking into account all potential factors prior to processing activities. The record of impact assessment should be connected to the duty of transparency according to the PIPL Articles 7, 14, and 48. As a new measure, compulsory disclosure of users' personal information with the aim of combating (mis) and (dis)information may change the original purposes and methods of processing personal information based on information subjects' initial consent and further exacerbate the power imbalance between platforms and information subjects. It is an essential practice for platforms to publish the process of impact assessment and any unexpected further use of the disclosed

[118] *See* CHENG, *supra* note 30, at 386–87.

information, such as profiling and behavioral targeting, or third parties with which it will share the disclosed information. The record would be conducive to notifying information subjects about how their data were collected, used, and shared.[119] Without knowing how disclosure might increase potential risks, users are placed in an unfair situation to continue their services.

3. Summary. In the test of proportionality in the narrow sense, platforms should holistically weigh the benefits gained by countering (mis) and (dis)information against the interference with the individuals' rights and interests related to personal information. The comparison could be conducted both absolutely – between the state of affairs before and after initiating the disclosure, and relatively – between marginal benefits and harms brought by both alternatives and the measure at issue.

If the measure is not proportionate, online platforms need to keep reworking the measure. During this process, providing additional safeguards according to the PIPL and our suggestions may reduce extra risks to information subjects brought by this measure. Notwithstanding, additional safeguards may not be a panacea. After the reassessment of proportionality, if the potential harm to personal information protection still outweighs the effectiveness of promoting public interest even with additional safeguards, terminating the proposed mandatory disclosure requirement would be the only way to comply with the requirement of "reasonable scope" in the PIPL Article 13 Paragraph 1(5).

V. CONCLUSION

Disclosing users' personal information on online platforms to counter (mis) and (dis)information may cause tensions between public interest and the protection of individual rights and interests over personal information. The sheer number of users and higher speed of dissemination in social media may further exacerbate this collision.

In this Note, we use the example of disclosing social media users' IP territoriality to argue that it is imperative to assess the legality of these measures within the framework of PIPL. By interpreting the definition of personal information, we argue that using pseudonyms as users' names will not take these measures out of the regulation of PIPL, because the disclosed users' personal information may still be indirectly identifiable and related to one natural person.

By examining multiple legal bases in Article 13, particularly Article 13 Paragraph 1(5), we elaborate on the framework of balancing public interests against personal information protection. When interpreting the "reasonable scope" in Article 13 Paragraph 1(5), policymakers and online platforms (i.e., personal information processors) should integrate the framework of propor-

[119] *See* Xinxi Anquan Jishu Geren Xinxi Anquan Yingxiang Pinggu Zhinan (信息安全技术 个人信息安全影响评估指南) [Information Security Technology – Guidance for Personal Information Security Impact Assessment] (promulgated by State Admin. for Market Regulation & Standardization Admin. of China, Nov. 19, 2020, effective Jun. 1, 2021), art. 4.3.

tionality, general principles, and the rules of personal information protection impact assessment in the PIPL to carefully confirm whether it is proportionate to disclose users' IP territoriality and what specific methods should be utilized. The permanent, non-targeted, and bulk disclosure of all users' IP territoriality without any detailed analysis of benefits and harms may not adequately demonstrate its proportionality. We suggest that online platforms should continuously assess the proportionality of disclosing users' personal information, not only because the *Provisions* Article 12 has granted wider discretion to online platforms to strike the delicate balance between competing rights and interests, but also because online platforms ought to respond to the dynamic and uncertain nature of social media and personal information protection immediately and responsibly.