UW-Google Intermediary Liability Research Project:

Privacy Protection in China
Abstract

In China, online privacy protection has gradually attracted increased attention amongst the public. In order to protect online privacy, specific statutes have been enacted by the legislature and case law has developed through judicial interpretations. Nevertheless, the public may not know how to protect their privacy or may lack the willingness to enforce their privacy on Internet. So far, there are a limited number of cases in which members of the public have sued online service providers ("OSPs") for online privacy infringement committed either by themselves or their users. Additionally, the rules governing identity disclosure are quite fragmented, and in different fields OSPs tend to follow different rules.

Principal investigator:
Prof. Yong Wan: KoGuan Law School, Shanghai Jiao Tong University.

Authors:
Jie Wang, PhD researcher at the Faculty of Law, Maastricht University; PhD candidate at Study Center for Intellectual Property, Zhongnan University of Economics and Law; Part II, Section 2.1; Part III.

Tianxiang He, PhD researcher at the Faculty of Law, Maastricht University; PhD candidate at Law School, Renmin University; Part II, Section 2.2.

Yaojin Peng, PhD researcher at the Faculty of Law, Maastricht University; Part I.
Introduction

In China, no specific, comprehensive law concerning privacy protection exists, and the rules governing privacy protection are fragmented. Traditionally, a right to privacy was recognized under a right of reputation. In 2010, China enacted the Tort Law of People’s Republic of China (hereafter Tort Law of China), which protects the right of privacy as an independent personal right parallel to right of reputation. Due to public concerns, the Tort Law of China contains provisions specifically regulating privacy protection on the Internet. Additionally, since online service providers ("OSPs") have access to Internet users’ private information, the authorities in China have also promulgated several regulations regulating the tracking, collection, utilization, and disclosure of private information on the Internet. This report aims to draw a full picture of online service provider’s responsibilities for privacy protection in China.

Outline of the Report:

In order to draw a full picture of OSP’s responsibilities for privacy protection in China, this report consists of three parts: (I) the general legal framework governing privacy protection in China, (II) OSP’s liability for privacy infringement, and (III) OSP’s obligation to disclose Internet users’ identity information. Part I begins by exploring some basic problems concerning privacy protection in China, including: whether privacy is an independent right, the contours of privacy rights, and what constitutes privacy infringement. Then, it explores OSP’s responsibilities for privacy protection prescribed in laws, regulations, and judicial interpretations in China. Part II presents case studies to demonstrate how Chinese courts determine OSP’s liability in cases involving privacy infringement. According to the different types of liability undertaken by online intermediaries, this part is divided into two sections examining direct liability and secondary liability. The section on direct liability examines whether the Chinese courts hold cookies tracking as privacy infringement. The section on secondary liability explores whether OSPs are liable for privacy infringement committed by...

---

1 In China, the rules governing privacy protection can be found in Constitution of People’s Republic of China, General Principles of the Civil Law of People’s Republic of China, Tort Law of People’s Republic of China, relevant judicial interpretations and administrative regulations. See Part I.

2 According to a series of Judicial Interpretations provided by People’s Supreme Courts, if the disclosure of privacy information causes damage to the victim’s reputation, the disclosure infringes the victim’s right to reputation. See infra Part I, Section 1.1.


4 Id, Article 36.

5 See part I, Section 1.2.
their users. Further, since the Internet is characterized by anonymity, in certain situations, online intermediaries may be required to help victims identify infringers. Part III examines case law concerning online intermediary’s obligations to disclose online identities in the fields of personal rights, copyright, and trademark. The conclusion summarizes the findings in the previous parts and then points out what needs to be further clarified by legislation and case law regarding privacy protection in China.

**Study Methodology:**

Part I examines the general legal framework of privacy protection by looking to the Chinese Constitution, statutes, judicial interpretations. Part II and Part III explore OSP’s responsibility to protect privacy through case studies and judicial opinions. In 2013, the People’s Supreme Court of China established a unitary platform called “Judicial Opinions of China” for the courts to publish their decisions. Since the beginning of 2014, all of the judicial opinions delivered by the Supreme Court, Higher Courts, Intermediate Courts and Local Courts in 13 provinces must be published on this platform. For cases decided before 2014, this report mainly relies on the scholarly database “Bei Da Fa Bao.” The authors believe that the analysis of case decisions collected from these two databases demonstrate how the Chinese courts interpret OSP’s responsibility to protect privacy.

Based on search results of these two databases, there are a limited number of cases in which plaintiffs sued OSPs for privacy infringement or requested that OSPs disclose Internet users’ identity information. Therefore, this report attempts to analyze all of the related case decisions collected from these two databases, which we believe helps draw a full picture of OSPs’ responsibility for privacy protection in judicial practice. When analyzing case decisions, the report adopts the following structure: facts, decision, and comments. Nevertheless, when discussing a complicated case which involves several key issues in dispute, the report structures the case study in light of key issues.

**Limitation:**

---


9 See Part II, Section 1.
As referenced above, there are a limited number of cases ruling on OSP’s responsibility for privacy infringement in China. Therefore, although this report tries to analyze all the related cases, there are still some provisions which need to be clarified but have not been interpreted by Chinese courts. Hence, the case study in this report is not capable of providing judicial insights into every provision related to OSP’s responsibility for privacy protection. In addition, although several laws and regulations grant authorities the power to conduct privacy enforcement on Internet, they do not clarify which authorities are competent to conduct such enforcement. Therefore, this report is also not capable of pointing out which authorities are responsible for privacy enforcement on Internet.
Part I. Legal Framework

Introduction

Traditionally, Chinese law did not emphasize protecting the privacy of natural persons. The Constitution does not set out any provisions directly concerning privacy. Moreover, the General Principles of the Civil Law of the People’s Republic of China (GPCL), which sets forth the legal basis for civil rights protection in China does not mention or protect privacy. China traditionally protected the privacy of natural persons through the right of reputation. Recent Chinese legislation explicitly creates a statutory right to privacy. For example, privacy is expressly mentioned in the Tort Law of China. Several other laws and regulations prevent privacy infringement and regulate online activities of OSPs. The first part of this report focuses on the applicable Chinese laws governing the liability of OSPs for infringing upon privacy. This part is divided into two sections: the legal framework of privacy protection and the corresponding liability of OSPs in China. Hopefully, this legal background examined in Part I forms the basis of the judicial decisions analyzed in Part II and Part III.

1.1 General Legal Structure of Privacy Protection

The first section of this part examines the question of whether privacy has become an independent right to be protected in China. Then, the legal basis is established. Lastly, an essential part of concluding liability for infringing upon privacy—causing damage—is examined.

(1) Privacy – Independent Right

Although it does not explicitly mention privacy, the Chinese Constitution does provide some basis for a right to privacy. The most relevant provision of the Chinese Constitution concerning privacy is Article 38, which states that “the personal dignity of citizens of the People’s Republic of China is inviolable. Insult, libel, false accusation or false incrimination...
directed against citizens by any means is prohibited.”\textsuperscript{12} This article enshrines the rights of reputation and personal dignity in the Constitution. Although this article does not explicitly provide for the protection of privacy, personal dignity can include privacy, which could constitute the basis of legislation and judicial interpretations protecting privacy in China.

In addition, Article 40 of the Constitution gives legal protection to the freedom and privacy (\textit{mimi}) of citizens’ correspondence. Specifically, Article 40 stipulates that “freedom and privacy of correspondence of citizens of the People’s Republic of China are protected by law. No organization or individual may, on any ground, infringe upon citizens’ freedom and privacy of correspondence, except in cases where, to meet the needs of State security or of criminal investigation, public security or procuratorial organs are permitted to censor correspondence in accordance with the procedures prescribed by law.” This article explicitly incorporates the privacy of citizens’ correspondence into the protective scope of the Constitution.

In addition to Constitutional protections, the General Principles of the Civil Law of the People’s Republic of China (GPCL) sets forth the legal basis for civil rights protection in China.\textsuperscript{13} However, the GPCL does not mention privacy, let alone the privacy protection. Article 101 of the GPCL merely provides a general right of reputation, which stipulates that:

\begin{quote}
\textbf{Natural persons and legal persons shall enjoy the right of reputation. The personality of citizens shall be protected by law, and the use of insults, libel or other means to damage the reputation of citizens or legal persons shall be prohibited.}\textsuperscript{14}
\end{quote}

This provision was further explained in Article 140 of the Opinions of the Supreme Court on Several Issues Concerning the Implementation of the GPCL (1988),\textsuperscript{15} which provides that:

\textsuperscript{12} Articles 38, 39 and 40 of the Chinese Constitution have been regarded as the constitutional basis for the legal protection of a right to privacy. Article 39 of the Constitution provides that “the residences of citizens of the People’s Republic of China are inviolable. Unlawful search of, or intrusion into, a citizen’s residence is prohibited.” However, Article 39 is not so relevant to liability of online intermediaries, and thus is beyond the discussion of this paper.
\textsuperscript{14} Article 101 of the GPCL.
In case any person discloses personal secrets in writing or orally, or fabricates facts to publicly vilify the personal dignity, or damages the reputation by such means as insults and defamation of the others, and these acts have caused a negative impact on the persons concerned, shall be treated as an invasion of the right to reputation.

Pursuant to this interpretation by the Supreme Court, a person is liable for disclosing the personal details of another when such a disclosure results in damage to the latter’s reputation, irrespective of whether this is done in verbal or written form. The 1988 Supreme Court Opinion has subsumed the concept of privacy into the terms “personal dignity” and “right of reputation.”

In a subsequent 1993 Supreme Court Interpretation, the Court states that “disclosing private information of others or broadcasting privacy of others in written or oral form without the consent of others, which leads to damage to reputation of others, shall be dealt with as an infringement of the reputation rights of others.” According to this interpretation of the Supreme People’s Court, a person is liable for infringing another’s reputation rights when their unpermitted disclosure of the other’s private information causes harm to the other’s reputation.

In addition, several other Chinese laws have been interpreted to protect the right to privacy. The Tort Law of China sets out a general imposition of tort liability in cases ranging from medical negligence, work-related injuries, and environmental pollution to product liability when the civil rights and interests of citizens are infringed. Article 2 of the Tort Law of China explicitly incorporated a right of privacy into “civil rights and interests,” which

---

16 The status of the Supreme People’s Court’s Interpretation is almost equivalent to legislation in form and nature. Different from common law system, the Supreme People’s Court in China has quasi-legislative and judicial interpretation functions. It has the ability of issuing guidelines on legal interpretation binding on lower courts, or policy guidelines to executive organs. Moreover, it is able to set forth legal principles in question-and-answer format for lower courts. For more discussion, see Albert Hy Chen, An Introduction to the Legal System of the People’s Republic of China 99-100 (Butterworths Asia. 1992).
18 Id. at 327. Rebecca Ong, Internet intermediaries: The liability for defamatory postings in China and Hong Kong, 29 COMPUTER L. & SECURITY REV. 274, 275 (2013).
21 Tort Law of China, supra note 3.
22 Article 2.2 of the Tort Law of China provides that “Civil rights and interests” used in this Law shall include the right to life, the right to health, the right to name, the right to reputation, the right to honor, right to self image, right of privacy,
means that the Tort law of China recognizes an independent right of privacy. Additionally, in the Law of the People’s Republic of China on the Protection of Women’s Rights and Interests, Article 42 prohibits any harm to women’s right to privacy by public media or otherwise.  

(2) Components of Privacy

Although there is no precise statutory definition of privacy, several forms of privacy are protected by Chinese laws and regulations. The privacy of medical patients is expressly protected in China. In the 1998 Interpretation of the Supreme Court Concerning the Right of Reputation, the Court indicated that a medical institution may bear tortious liability if a patient’s reputation is harmed by the institution’s unauthorized revelation of certain medical illnesses. Specifically, Question and Answer VIII of this interpretation holds that “where a staff member of a medical and hygiene institution illegally discloses that a patient is suffering from gonorrhea, syphilis, leprosy, AIDS, et., if the patient’s right of reputation is thus damaged, it will constitute an infringement on the patient’s right or reputation.” Moreover, the privacy of patients is further protected under Article 62 of the Tort Law of China, which states that “a medical institution and its medical staff shall keep confidential the privacy of a patient. If any privacy data of a patient is divulged or any of the medical history data of a patient is open to the public without the consent of the patient, causing any harm to the patient, the medial institution shall assume the tort liability.”

Recent Chinese laws and regulations have expanded protections beyond medical patients, protecting the basic personal information of all citizens. A 2013 regulation, jointly issued by the Supreme Court, Supreme Procuratorate, and Ministry of Public Security, provides that “the personal information of citizens includes the name, age, valid certificate number, marital autonomy, guardianship, ownership, usufruct, security interest, copyright, patent right, exclusive right to use a trademark, right to discovery, equities, right of succession, and other personal and property rights and interests.

23 Zhonghua Renmin Gonghe Guo Funü Quanyi Baozhang Fa (中华人民共和国妇女权益保障法) [Law of the People’s Republic of China on the Protection of Women’s Rights and Interests] (promulgated by the 5th Session of the Seventh National People’s Congress, Apr. 3, 1999, amended according to the Decision of the 17th Session of the Standing Committee of the Tenth National People’s Congress about Amending the Law of the People’s Republic of China on the Protection of Women’s Rights and Interests, Aug. 28, 2005). Article 42 provides that “(1) women’s personal rights, such as right of reputation, right of honor, right of privacy, and right to portrait shall be protected by law. (2) It is prohibited to injure women’s reputation or personal dignity by insult, slander, etc. It is prohibited to debase or injure women’s personal dignity by public media or otherwise. Without a woman’s own permission, it is prohibited to use her portrait in advertisements, trademarks, window display, newspapers, periodicals, books, audio-visual products, electronic publications, internet, etc.”

24 Zuigao Renmin Fayuan Guanyu Shenli Mingyu Anjian Ruogan Wenti de Jieshi (最高人民法院关于审理名誉权案件若干问题的解释) [Interpretation of the Supreme People’s Court on Several Issues about the Trial of Cases Concerning the Right of Reputation], FS [1998] No. 26 (promulgated by the 1002nd Meeting of the Judicial Committee of the Supreme People’s Court, July 14, 1998, effective Sept. 15, 1998) available at http://en.pkulaw.cn/display.aspx?cgid=20791&lib=law (last visited Aug. 4, 2015). (last tionn.list involving e at nli Guiding e Ruogan Wenti de Yijian paper.e 38. the right privacy.inate the following informa
status, employer, education background, resume, family address, phone number and other information or data that can identify the identities of citizens or involve the personal privacy.”

A similar statement can be found in Article 4 of the Provisions on Protecting the Personal Information of Telecommunications and Internet Users (2013), which states that “users’ personal information means a user’s name, date of birth, identity card number, address, telephone number, account number, passwords and other information with which the identity of the user can be distinguished independently or in combination with other information, as well as the time, and place of the user using the service and other information, as collected by telecommunications service operators and Internet information service providers in the process of providing services.”

Moreover, Article 12.1 of the Provisions of the Supreme Court on Several Issues concerning the Application of Law in the Trial of Cases involving Civil Disputes over Infringements upon Personal Rights and Interests through Information Networks (hereafter Provisions on Online Infringement of Personal Rights) provides that “where a network user or network service provider discloses through network a natural person’s individual privacy such as genetic information, medical records, health inspection materials, criminal records, home address, and private activities, or any other personal information, which causes damage to any other person, and the infringed party requests the assumption of tort liability by the network user or network service provider, the people’s court shall support such a request.”


26 Dianxin he Hulian Wang Yonghu Geren Xinxi Baohu Guiding (电信和互联网用户个人信息保护规定) [Provisions on Protecting the Personal Information of Telecommunications and Internet Users] (promulgated by the Ministry of Industry & Information Technology, July 16, 2013). Actually, the Provisions on Protecting the Personal Information provides a comparatively comprehensive regulatory guideline with regard to collecting and using Internet users’ personal information by the OSP. The 2013 Provisions lay down basic principles that OSPs should follow when they are collecting and using users’ personal information, namely the principles of legality, propriety and necessity. The OSP is required to formulate the rules for collection and use of users’ personal information and publish such rules on its website. Without the consent of users, the OSP may not collect and use users’ personal information. More importantly, the OSP is expressly required to strictly keep confidential users’ personal information collected and used by the OSP in the process of providing services, and not to divulge, alter, destroy, sell, or illegally provide others with such information.

27 Zuigao Renmin Fayuan Guanyu Shenli Liyong Xinxi Wangluo Qinhai Renshen Quanyi Minshi Jiufen Anjian Shiyong Ruogan Wenti de Guiding (最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定) [Provisions of the Supreme People’s Court on Several Issues concerning the Application of Law in the Trial of Cases involving Civil Disputes over Infringements upon Personal Rights and Interests through Information Networks], Interpretation No. 11 [2014] (promulgated by the 1,621st session of the Judicial Committee of the Supreme People’s Court, June 23, 2014, effective Oct. 10, 2014) available at http://en.pkulaw.cn/display.aspx?cgid=235297&lib=law (last visited Aug. 4, 2015). Article 1 of this Interpretation provides a list of types of cases that the courts should accept, including those cases involving disputes arising from the infringements over any other person’s right of … reputation, … or privacy through information networks.
Concerning the dissemination of personal information that may involve OSPs, Article 12.2 of the Provisions on Online Infringement of Personal Rights provides a list of several liability exemptions, namely “(1) the natural person has agreed in writing and publication takes place within the scope of the agreements; (2) in order to spur the social public interest, and it is within the scope of necessity; (3) by schools, scientific institutions, etc., for the purposes of scientific research for the public interest, or for statistical purposes, with the written agreement of the natural person, and the method of publication does not allow the identification of a specific natural person; (4) where natural persons themselves publish this information online or other personal information that is already lawfully published; (5) personal information that is obtained through lawful channels; (6) except where laws or administrative regulations provide otherwise.”

However, if the OSP discloses personal information as provided in Items 4 and 5 listed above in a manner that violates the social public interest or social morality, or the disclosure of the information concerned harms major interests of rights holders that merit protection, the OSP may bear tort liability.

(3) Causing Damage – An Essential Part of Determining Liability

One common feature of the privacy protections found in laws, regulations, and judicial opinions is that the mere disclosure of private facts may not be actionable unless the disclosure results in harm to the injured party. In other words, unless the person can show the damage to reputation caused by the public disclosure of private information, one may not be capable of bringing an independent action for privacy infringement. For example, Article 140 of the Opinions (1988) requires that “…these acts have caused a negative impact on the persons concerned…” In the 1993 Interpretation, it provides that “…which leads to damage to reputation of others…” In Article 62 of the Tort Law of China, it stipulates that “…causing any harm to the patient…” Thus, providing damage to the plaintiff has become one extremely significant perquisite for bringing a privacy infringement claim.

Moreover, the damage to the victim can be mental damages. For instance, pursuant to Article 1.2 of the Interpretation of the Supreme Court on Problems regarding the Ascertainment of Compensation Liability for Emotional Damages in Civil Torts (2001), “the court shall accept cases arising from the violation of societal public interests or societal morality by infringing upon a person’s privacy or other interests of personality, and brought to the court by the

---

28 Article 12.2 of the Provisions on Online Infringement of Personal Rights.
29 Article 12.3 of the Provisions on Online Infringement of Personal Rights
victim as a civil tort for claiming emotional damages.” 30 Furthermore, Article 22 of the Tort Law of China stipulates that “where any harm caused by a tort to a personal right or interest of another person inflicts a serious mental distress on the victim of the tort, the victim of the tort may require compensation for the infliction of mental distress.” 31

In summary, the General Principles of the Civil Law, one of the most significant laws in China, sets out the legal basis for civil rights protection, but does not specifically mention privacy or the right of privacy. However, several judicial interpretations have subsumed the concept of privacy into the terms “personal dignity” and “right of reputation.” Several other laws and regulations have given additional protection to privacy. Particularly, the Tort Law of China has incorporated the right of privacy into its protection, but it still does not give any definition of the right of privacy or privacy. Thus, the parameters of the right of privacy in China still remain unclear.

1.2 Specific Legal Structure Concerning Online Service Providers

In China there is no overarching legislation concerning liability of OSPs, and there are vast OSP-related provisions existing in fragmented laws and regulations. Thus, the analysis of this section does not go very far, but mainly focuses on rules concerning liability of the OSP for infringing upon privacy and rules that the Chinese government has issued which aim to regulate the OSP.

(1) Rules Concerning Intermediaries Liability of the OSP

The first major provision involving the liability assumed by OPSs is Article 36 of the Tort Law of China, which specifically applies to online torts and is referred to as the Internet Clause. 32 This article stipulates circumstances in which the OSP can be found liable. It expressly categorizes the liability of the OSP into direct liability and secondary liability, 33 which sets out that:


31 Tort Law of China, supra note 3, Article 22.


33 Zuigao Renmin Fayuan Fu Yuanzhang Xi Xiaoming Zai Quanguo Fayuan Zhishi Chanquan Shenpan Gongzuo Zhongye Shang de Jianghua (最高人民法院副院长奚晓明在全国法院知识产权审判工作座谈会上的讲话——能动司法，服务大
A network user or network service provider who infringes upon the civil right or interest of another person through network shall assume the tort liability. Where a network user commits a tort through the network services, the victim of the tort shall be entitled to notify the network service provider to take such necessary measures as deletion, block or disconnection. If, after being notified, the network service provider fails to take necessary measures in a timely manner, it shall be jointly and severally liable for any additional harm with the network user. Where a network service provider knows that a network user is infringing upon a civil right or interest of another person through its network services, and fails to take necessary measures, it shall be jointly and severally liable for any additional harm with the network user.\textsuperscript{34}

Article 36.1 imposes direct liability on the OSP when the OSP is directly engaged in infringing upon the civil rights and interests of others. The other two paragraphs of Article 36 set out two circumstances in which the OSP assumes secondary liability.\textsuperscript{35} Article 36.2 is essentially a “safe harbor” rule, where the OSP is merely liable for additional damage that is caused by not taking down the claimed unlawful information provided by network users in a timely manner upon notification.\textsuperscript{36}

In terms of the forms of notice provided in Article 36.2 of the Tort Law of China, the Provisions on Online Infringement of Personal Rights (2014) further explain that “the notice sent to an OSP by the infringed party in writing or in the manner announced by the OSP contains the following contents, the court shall determine such a notice as valid. (1) The name (title) and contact information of the informant. (2) The network address against which necessary measures shall be taken as required or the relevant information sufficient enough to determine the infringement. (3) The grounds of the informant for deleting the relevant information. Where the notice sent by the infringed party fails to meet the aforesaid conditions, and the OSP claims the exemption of liabilities, the people’s court shall support

\textsuperscript{34} Tort Law of China, supra note 3, Article 36.
\textsuperscript{35} Article 3 of Provisions on Online Infringement of Personal Rights (2014) further stipulates that “(1) where the plaintiff files a lawsuit against a network user or network service provider in accordance with paragraphs 2 and 3, Article 36 of the Tort Law, the people’s court shall accept such a lawsuit. (2) where the plaintiff only files a lawsuit against the network user, and the network user requests the people’s court to add the network service provider suspected of infringement as the co-defendant or the third party, the people’s court shall approve such a request. (3) where the plaintiff only files a lawsuit against the network service provider, and the network service provider requests the people’s court to add the network user that may be determined as the co-defendant or the third party, the people’s court shall approve such a request.” See supra note 27.
\textsuperscript{36} Xiaoming, supra note 33.
such a claim.” 37 However, according to this Article of the Interpretation, it is still unclear whether notification by a third party is adequate notice, which may considerably influence the exemption of liabilities that the OSP claims.

Regarding the takedown of information, including deletion, blocking or disconnection provided in Article 36.2 of the Tort Law of China, the Provisions on Online Infringement of Personal Rights (2014) explain that whether necessary measures are taken by the OSP in a timely manner shall comprehensively be judged based on: the nature of network services, the form and degree of accuracy of effective notice, the type and extent of rights and interests infringed upon by the network information, and other factors. 38 Moreover, Article 7 of the Provisions on Online Infringement of Personal Rights (2014) further explains that “where a network user against whom the measures such as information deletion, block and disconnection are taken claims that the OSP shall assume the liability for the breach of contract or tort liability, and the OSP makes a defense on the ground of receiving a notice, the people’s court shall support such a claim. Where a network user against whom the measures such as information deletion, block and disconnection are taken claims the OSP shall provide the notified contents, the people’s court shall support such a claim.” 39 Based on this provision, it could likely lead to a situation that the OSP is inclined to take necessary measures to take down the potentially unlawful content as long as the OSP receives the effective notice, irrespective of whether or not the content really infringes upon privacy of others.

Article 36.3 of the Tort Law of China provides a knowledge test for the imposition of liability, potentially holding an OSP liable if they “actually knew” or “should have known” that such information was private. 40 Regarding determining whether the OSP “knows”, the Supreme People’s Court has pointed out several factors, including “(1) whether the OSP handles the infringing network information manually or automatically by such means as recommendation, ranking, selection, editing, review and amendment; (2) the required information management capability of the OSP, and the nature, form and possibility of infringement of services provided by the OSP; (3) The type and obviousness of the network information’s infringement upon personal rights and interests; (4) the social impact of such network information or page view within a certain time; (5) technical possibility of

37 Provisions on Online Infringement of Personal Rights (2014), supra note 27, Article 5.
39 Id.
40 Xiaoming, supra note 33.
infringement prevention measure taken by the OSP and whether the corresponding reasonable measure has been taken; (6) whether the OSP has taken the corresponding reasonable measures against the repeated infringements or the same infringing information of the same network user; and (7) other factors relating to this case.”41

In terms of an obligation for the OSP to cease transmission of information which infringes upon the right of privacy, it is worth noting Article 7 of the Decision of the Standing Committee of the National People’s Congress Concerning Maintaining Internet Security (2000). This article requires that service providers not only to cease transmission of any harmful message on the Internet, but also report such matter to authorities.42 Specifically, Article 7 of this decision provides that “…any unit that engages in the computer network business shall carry out activities in accordance with law and, when it discovers illegal or criminal acts or harmful information on the computer network, shall take measures to suspend transmission of harmful information and report the matter to the relevant authority without delay…”

Moreover, the Standing Committee of the National People’s Congress has issued another Decision (2012), which involves strengthening information protection on networks.43 It comprehensively gives legal protection of individual privacy of citizens online in China.

Article 1 (1) The state protects electronic information by which individual citizens can be identified and which involves the individual privacy of citizens.
(2) All organizations and individuals may not obtain electronic personal information of citizens by theft or any other illegal means and may not sell or illegally provide others with electronic personal information of citizens.

Article 2 (1) The OSP and other enterprises and institutions shall, when gathering and using electronic personal information of citizens in business activities, adhere to the principles of legality, rationality and necessarily, explicitly state the purposes, manners and scopes of collecting and using information, and obtain the consent of those from whom information is

41 Provisions on Online Infringement of Personal Rights (2014), supra note 27, Article 9.
43 Quanguo Renda Changweihui Guanyu Jiaqiang Wangluo Xinxi Baohu de Jueding (全国人大常委会关于加强网络信息保护的决定) [Decision of the Standing Committee of the National People’s Congress on Strengthening Information Protection on Networks] (promulgated by the Standing Committee of the National People's Congress, Dec. 28, 2012).
collected, and shall not collect and use information in violation of laws and regulations and the agreement between both sides. (2) The OSP and other enterprises and institutions shall, when gathering and using electronic personal information of citizens, publish their collection and use rules.

Article 3 The OSP and other enterprises and institutions and their personnel must strictly keep confidential and may not divulge, alter, damage, sell, or illegally provide others with the electronic personal information of citizens gathered in business activities.

Article 4 The OSP and other enterprises and institutions shall take technical measures and other necessary measures to ensure information security and prevent electronic personal information of citizens gathered in their business activities from being divulged, damaged or lost. When any information divulgence, damage or loss occurs or may occur, remedial actions shall be taken immediately.

Article 5 The OSP shall strengthen management of information released by their users and, when discovering any information prohibited by laws and regulations from being released or transmitted, immediately stop the transmission of such information, take elimination and other handling measures, preserve relevant records, and report to the relevant competent authorities.

Article 8 Citizens who discover any network information divulging their personal identities, disseminating their individual privacy or otherwise infringing upon their lawful rights and interests or who are annoyed by unwanted commercial electronic information shall have the right to require the OSP to delete relevant information or take other necessary prohibitive measures.

In addition to legal protection of privacy that Chinese legislations provide in civil law, practical protection of privacy also can be found in criminal law. For example, there is one article in the Criminal Law of China potentially relevant to personal privacy protection concerning the OSP, Article 253. This article states that:

44 Zhonghua Renmin Gonghe Guo Xingfa (中华人民共和国刑法) [Criminal Law of the People's Republic of China] (promulgated by the Second Session of the Fifth National People's Congress, July 1, 1979, and promulgated by Order No.5
Where any staff member of a state organ or an entity in such a field as finance, telecommunications, transportation, education or medical treatment, in violation of the state provisions, sells or illegally provides personal information on citizens, which is obtained during the organ’s or entity’s performance of duties or provision of services, to others shall, if the circumstances are serious, be sentenced to fixed-term imprisonment not more than three years or criminal detention, and/or be fined.

Whoever illegally obtains the aforesaid information by stealing or any other means shall, if the circumstances are serious, be punished under the preceding paragraph.

Where any entity commits either of the crimes as described in the preceding two paragraphs, it shall be fined, and the direct liable person in charge and other directly liable persons shall be punished under the applicable paragraph.\(^{45}\)

This provision may bring the OSP into the scope of criminal liability for infringing upon privacy of others.

(2) Rules Towards Governing the OSP

Aside from laws, the Chinese government has issued several additional regulations to ensure that online activities of the OSP are controlled. These regulations prohibit any insulting or defamatory information against others or any infringement upon the legal rights and interests of others in the cyber world. For example, one of the early regulations issued by the Chinese government to regulate the posting and dissemination of defamatory and harmful content is the Measures for Security Protection Administration of the International Networking of Computer Information Networks approved by the Chinese State Council in 1997.\(^{46}\) The rules

\(^{45}\) According to Article 7 of the Amendment (VII) to the Criminal Law of the People’s Republic of China, these provisions have been inserted after Article 253 of the Criminal Law. See Zhonghua Renmin Gonghe Guo Xingfa Xiuzheng An (Qi) (中华人民共和国刑法修正案(七)) (Amendment (VII) to the Criminal Law of the People’s Republic of China) (promulgated by the 7th session of the Standing Committee of the 11th National People’s Congress of the People’s Republic of China, Feb. 28, 2009, effective Feb. 28, 2009).

mainly prescribe the registration of users before using the Internet and point out several prohibitive online activities, such as using the Internet to create falsehoods, distort the truth, spread rumors, openly insult others, distort the truth to slander others.\textsuperscript{47} Moreover, in the Regulation on Internet Information Service (2000), Article 15 explicitly prohibits online service providers from creating, duplicating, releasing or disseminating content that insults or defames others or infringes upon the lawful rights and interests of others.\textsuperscript{48} Article 57 of the Telecommunication Regulation (2000),\textsuperscript{49} and Article 19 of Provisions for the Administration of Internet News Information Services (2005),\textsuperscript{50} respectively, stipulate that service providers are not permitted to release any information which insults or defames others or infringes upon the lawful rights and interests of others.

In addition, other regulations place affirmative duties on OSPs. These regulations affirmatively require OSPs to keep record of relevant data concerning the providing of information, cease transmission of infringing information, keep record of such information, report the alleged unlawful information to authorities, and provide the addresses of Internet users who have visited their site to the proper authorities. For example, Article 10 of the Measures for Security Protection Administration of the International Networking of Computer Information Networks requires all OSPs and access providers to register the units and individuals that entrust them to publish information, remove the unlawful content, cease transmission, and submit a report to the local public security organ within 24 hours.\textsuperscript{51} Article 16 of the Regulation on Internet Information Service requires service providers to immediately cease the distribution and transmission of unlawful and harmful information, record such information, and report to the proper authorities.\textsuperscript{52}

\textsuperscript{47} Id. Article 5 of of this Regulation provides that “no unit or individual shall use the international networking to produce, duplicate, search and disseminate the following information: … (7) information that openly indults others or fabricates facts to slander others; … (9) other information that violates the Constitution, laws and administrative regulations.”


\textsuperscript{51} Measures for Security Protection Administration of the International Networking of Computer Information Networks, supra note 46, Article 10.

\textsuperscript{52} Regulation on Internet Information Service, supra note 48, Article 16. In terms of keeping record of relevant data, Article 14 of this Regulation expressly requires an Internet information service provider who provides news, publication or electronic bulletin boards to keep records of the information it provides, the publishing date and the Internet address or domain name. It also requires an Internet information service provider who provides service of Internet connection to keep...
the Provisions for the Administration of Internet News Information Services (2005) requires Internet news information service providers to record information and keep back-up copies of information for 60 days, such as content provided, publishing times, and Internet addresses. The information shall be provided to State authorities when required to do so.\(^{53}\) Moreover, Article 18 of the Administrative Provisions on Internet Audio-Visual Program Service (2008) requires all Internet audio-visual program service providers to immediately remove unlawful content, keep relevant records, and report violations to the authorities.\(^{54}\)

Furthermore, recently the Chinese government has issued another regulation specific to OSPs. This regulation again requires the OSP to follow several rules so as to ensure that the collection and use of users’ personal information online will not be abused. Specifically, the Provisions on Protecting the Personal Information of Telecommunications and Internet Users (2013) has provided several provisions to regulate the collection and use of users’ personal information in the process of providing telecommunications services and Internet information services.\(^{55}\)

**Article 5** Telecommunications service operators and Internet information service providers shall, when collecting and using users’ personal information in the process of providing services, adhere to the principles of legality, propriety and necessity.

**Article 6** Telecommunications service operators and Internet information service providers shall be responsible for the security of users’ personal information collected and used by them in the process of providing services.

**Article 9** Without the consent of users, no telecommunications service operator or Internet information service provider may collect and use users’ personal information.

**Article 10** Telecommunications service operators and Internet information service providers and their staff members shall strictly keep confidential users’

---

\(^{53}\) Provisions for the Administration of Internet News Information Services, supra note 50, Article 20-21. Concerning when and by what protocols OSPs are required to provide information to related authorities, please see infra Part II.

\(^{54}\) Hulian Wang Shiting Jiemu Fuwu Guanli Guiding (互联网视听节目服务管理规定) [Administrative Provisions on Internet Audio-Visual Program Service] (promulgated by the State Administration of Radio, Film and Television and the Ministry of Information Industry of the People’s Republic of China, effective Jan. 31, 2008). Article 16 of this regulation also gives a list involving unlawful content, which includes insulting, defaming other people and infringing the privacy information.

\(^{55}\) Provisions on Protecting the Personal Information of Telecommunications and Internet Users, supra note 26.
personal information collected and used by them in the process of providing services, and shall not divulge, alter, destroy, sell, or illegally provide others with such information.

Article 12 Telecommunications service operators and Internet information service providers shall establish the mechanisms for handling users’ complaints, publicize effective means of contact, accept all complaints related to the protection of users’ personal information, and give replies to complainants within 15 days after the complaints are accepted.

Article 13 Telecommunications service operators and Internet information service providers shall take the following measures to prevent the divulgence, destruction, alteration or loss of users’ personal information: (1) Determining the security management responsibilities among various departments, posts and branches for users’ personal information; (2) Establishing the workflows and security management systems for collection and use of users’ personal information and other relevant activities; (3) Administering the authorities of staff members and agents, examining the channeling, reproduction and destruction of information, and taking anti-phishing measures; (4) Properly keeping the paper, optic, electromagnetic and other media that record users’ personal information, and taking corresponding security storage measures; (5) Reviewing the access to the information systems which store users’ personal information, and taking anti-invasion, anti-virus and other measures; (6) Recording the personnel operating users’ personal information, and the time, places, matters and other information thereof; (7) Conducting the communication network security protection work in accordance with the provisions of telecommunications administrative organs; and (8) Other necessary measures as specified by telecommunications administrative organs.

Article 14 (1) Where users’ personal information under the custody of telecommunications service operators and Internet information service providers is or may be divulged, destructed or lost, remedial measures shall be taken immediately. Where serious consequences are or may be caused, they shall immediately report to the telecommunications administrative organs which issued their licensing or approved their registration, and cooperate with the relevant departments in investigation and handling.
In summary, in accordance with Chinese laws, the OSP may be held liable if they infringe a privacy right or interest of others, and the liability generally can be divided into two categories, direct liability and secondary liability. If the OSP illegally reveals others’ private information, it may assume direct infringement liability. Chinese laws and regulations have expressly stipulated several provisions to prohibit the OSP from disclosing or transmitting privacy information of others illegally, and require the OSP to keep its users’ personal information. If the circumstances are serious, the OSP may assume criminal liability. Moreover, if the service system of the OSP is employed for privacy infringement by its users, the OSP may be found to assume secondary infringement liability. This secondary liability applies when the OSP fails to fulfill a certain duty of care to prevent the privacy infringement from occurring. Meanwhile, Chinese legislation has also set out several duties of care for the OSP, such as ceasing transmission the infringing information, keeping records, and reporting misconduct to authorities.

1.3 Conclusion

The legal framework concerning privacy protection, as described in this Part, tells us that the right to privacy has been regarded as an independent right in China. Whilst there are several major statutes or regulations recognizing privacy protection in China, there is no overarching privacy legislation.56 There is no specific, comprehensive law or regulation establishing the liability of the OSP for privacy infringement. In other words, China relies on various fragmented laws, regulations and judicial decisions to protect privacy and the right of privacy, and to impose the liability of the OSP when privacy is directly or indirectly infringed. In addition, the regulatory framework is similarly fragmented, as legislation broadly grants enforcement authority to “relative authorities.”. Thus, there are several legal authorities, which have the competence to regulate the OSP when the OSP is suspected of involvement in infringing upon privacy rights and interests of others, such as people’s courts, local public security organs, telecommunications administrative organs. However, whether other authorities are also competent to enforce privacy protection is still unclear.

Recently, an increasing number of laws and regulations have been issued in China to regulate the infringement of privacy online, which suggests that the Chinese legislature has begun paying more attention to this field. At the same time, the Chinese legislation has concurrently regulated the activities of the OSP. Many representatives of National People’s Congress have

submitted several legislative proposals concerning developing online protection law of personal information or protection law of privacy rights and interests at the meeting of National People’s Congress. At the same time, the Legislative Affairs Commission has already taken these issues into consideration, reflected by the Network Security Law of China. This evidently suggests that China has paid more attention to privacy protection generally and further emphasized the importance of privacy protection online. Thus, it should not be difficult to predict that in China increasing and more comprehensive legislation concerning the liability of the OSP for infringing upon privacy or the right of privacy will come out.

57 The Law Committee of National People’s Congress issued a report passed by the 11th Standing Committee of the National People’s Congress in the 6th Meeting on December 27, 2008. In this report, No. 336 proposal pointed out to formulate the online privacy protection law, available at http://www.npc.gov.cn/wxzl/gongbao/2009-02/05/content_1505250.htm (last visited Aug. 1, 2015); Chen Jiyan and other 31 representatives put forward a proposal (No. 298) concerning formulating the privacy rights and interests protection law at the 11th Standing Committee of the National People’s Congress in the 2nd Meeting on Mar. 27, 2009, available at http://www.npc.gov.cn/wxzl/gongbao/2009-06/10/content_1517220.htm (last visited Aug. 1, 2015); Zhou Xiaoguan and other 29 representatives put forward a proposal (No. 362) concerning formulating the Internet shopping law, including protecting online privacy, at the 11th Standing Committee of the National People’s Congress in the 2nd Meeting on Oct. 31, 2009, available at http://www.npc.gov.cn/wxzl/gongbao/2009-12/15/content_1543817.htm (last visited Aug. 1, 2015); Chen Jiyan and other 31 representatives put forward a proposal (No. 459) at the 11th Standing Committee of the National People’s Congress in the 42th Meeting on Oct. 31, 2009. They proposed to make clear the definition, general principle, and main content of the right of privacy. Moreover, there were other three proposals (No. 25, No. 206, and No. 558) concerning formulating personal information protection law, and a proposal (No. 152) regarding privacy protection law, available at http://www.npc.gov.cn/wxzl/gongbao/2012-03/06/content_1705043.htm (last visited Aug, 1, 2015).

58 In June, 2015, the 15th Meeting of the 12th Standing Committee of the National People’s Congress preliminarily reviewed the Internet Security Law (draft), and right now is soliciting advice from the general public.
Part II: OSP’s Responsibility of Privacy Protection – a Case Law Perspective

According to the legal framework of privacy protection introduced in Part I, Internet intermediaries in China may be held liable for violating rules and regulations protecting privacy. As the laws governing privacy protection of Internet intermediaries have developed recently, there are a limited number of Chinese cases interpreting the effects of direct and secondary liability. Regarding direct liability, if an Internet intermediary illegally discloses its users’ privacy information on its own, it may commit a direct infringement against the users’ privacy.59 By contrast, if an Internet intermediary’s service is used for privacy infringement by its users, and fails to fulfill certain duty of care to prevent the privacy infringement from occurring, it may be found secondarily liable for the privacy infringement committed by its users.60

Regarding direct liability, to this point, Internet intermediaries in China have not been sued for directly infringing Internet users’ privacy except in a dispute about cookies tracking. As for secondary liability, there have been several cases in which plaintiffs sued Internet intermediaries for privacy infringement committed by their users. Part II therefore contains two sections examining (1) direct liability and (2) secondary liability. In the section of direct liability, since so far there exists only one case dealing with cookies tracking, this section mainly focuses on a discussion of this case. In the section of secondary liability, it discusses all relevant cases that we can find on the http://www.court.gov.cn/zgcpwsw/.

2.1: Direct Liability

“Cookies were designed to be a reliable mechanism for websites to remember stateful information (such as items in a shopping cart) or to record the user's browsing activity (including clicking particular buttons, logging in, or recording which pages were visited by the user as far back as months or years ago).”61 Nowadays, cookies, especially third party cookies, are used for tracking Internet users’ browsing history so as to provide personalized advertising.62 Since third party cookies track Internet users’ complete browsing history, it may arouse public concerns about privacy. However, In China, Internet users have not

59 See Tort Law of China (侵权责任法), supra note 3, Article 36.
60 Id.
expressed major concerns over cookies tracking, as there has only been one case involving this issue.\(^{63}\)


2.1.1. Facts

In this case, Baidu v. Zhu Ye, the defendant Baidu is the largest search engine operator in China. Baidu employs cookie tracking technologies to provide personalized advertising services to third party advertisers. At the bottom of Baidu’s main webpage, there is a hyperlink that reads: “Baidu read before use.” After clicking this hyperlink, users can find the Declaration on Privacy Protection (an internally developed corporate policy), which states that Baidu may track the users’ cookies for the purpose of optimizing its advertising service. Further, the declaration also states that users can reject the cookie tracking, and offers several ways for the users to disable the cookie tracking. The plaintiff Zhu Ye found, after searching information in Baidu with key words, some websites would display an advertisement related to the key words when she viewed these websites. Therefore, the plaintiff claimed that Baidu recorded and tracked the key words searched by her without her knowledge and permission, which led to the plaintiff’s interests, hobbies, and living, learning, and working habits being exposed on the websites. Further, the plaintiff also claimed that the defendant delivered the personalized advertisement to her by using the records of her searching history, so the defendant infringed her privacy.

2.1.2. Dispute One: whether third party cookie belongs to personal privacy

Regarding whether third party cookie belongs to personal privacy, the courts in two instances delivered different opinions.\(^{64}\) According to the Court of first instance, because third party cookies record the history of personal activity on the Internet and can reveal the users’ interests, habits, and other personal information, it held that third party cookies are protected as a part of personal privacy. By contrast, the Court of second instance reversed this

\(^{63}\) The Final Instance of the First Case on Cookies: the Court held that the Personalized Advertising was not infringing (Cookie第一案终审：法院判定个性化推荐不侵权), http://tech.qq.com/a/20150612/051726.htm, (last visited Aug. 4, 2015).

\(^{64}\) In China, the Court of First Instance is similar to a trial court in the US, and the Court of Second Instance is similar to an appellate court in the US. In addition, the Court of Second Instance makes final judgement.
determination, holding that third party cookies are not part of a users’ protected personal privacy. In light of Provisions on Protecting the Personal Information of Telecommunications and Internet Users prescribed by the Ministry of Industry and Information, “users’ personal information” includes a user’s name, date of birth, identity card number, address, telephone number, account number, passwords and other information with which the identity of the user can be distinguished independently or in combination with other information, as well as the time and place of the user using the service and other information, as collected by telecommunications service operators and Internet information service providers in the process of providing services. Based on this Article, the Court of second instance held that to be protected, personal information must be able to identify individual internet users. Although third party cookies record the Internet users’ online activity history and reflect their surfing preferences, which embody many characteristics of privacy, if this information is isolated from the Internet users’ identities, it is no longer part of users’ personal information. Since third party cookies are only targeted at communicating with users’ browsers but are not capable of having the users identified, they do not belong to the personal information.

2.1.3. Dispute two: whether Baidu infringes the users’ privacy

Regarding what constitutes privacy infringement, the courts of two instances also delivered different opinions. The Provisions on Online Infringement of Personal Rights states that an Internet intermediary can be found liable in tort for privacy infringement if: (1) the intermediary discloses through network a natural person’s individual privacy such as genetic information, medical records, health inspection materials, criminal records, home address, private activities, or any other personal information; (2) this disclosure causes damage to the person; (3) and the infringed party requests the assumption of tort liability by the network user or OSP.

The court of the first instance held that although Baidu did not disclose the plaintiff’s online activity, the collection and utilization of the plaintiff’s personal information was sufficient to conclude that Baidu infringed the plaintiff’s privacy. By contrast, the court of the second instance strictly followed the literal meaning of this Article, and held only the disclosure of privacy information constituted privacy infringement. In this case, the defendant Baidu did not disclose the information it collected through Cookies to third parties or the public, so

---

65 Provisions on Protecting the Personal Information of Telecommunications and Internet Users, supra note 26, Article 4.
66 Provisions on Online Infringement of Personal Rights, supra note 27, Article 12.
Baidu did not commit privacy infringement as defined by the Provisions on Infringing Rights of Person.

2.1.4. Dispute 3: whether Baidu fulfils the obligations of ensuring users’ rights to know and choose

As referenced in the facts section, at the bottom of Baidu’s main webpage, there is a hyperlink which reads: “Baidu read before use”. After clicking this hyperlink, users can find the Declaration on Privacy Protection, which states that Baidu may track users’ cookies for the purpose of optimizing its advertising services. Further, the declaration also states the users can reject the cookie tracking, and offers several ways for the users to disable the cookie tracking. The courts of two instances delivered different opinions on whether the above efforts fulfill the OSP’s obligation of ensuring users’ right to know and choose. According to the court of the first instance, Baidu collected and utilized its users’ surfing information without the users permission beforehand, and users probably did not know their personal information was collected and utilized. Therefore, Baidu was held to the higher standard of affirmatively notifying users of the collection of cookie information to allow them to make reasonable choices. Further, because the “Baidu read before use” notification was displayed at the bottom of the webpage in small font, it was not an effective notice to users.

By contrast, the courts of the second instance held Baidu fulfilled their notifying obligation. First, cookie tracking technologies are commonly employed by Internet companies, so it was sufficient for Baidu to notify users that these technologies were employed in the disclaimer at the bottom of the web page. Further, the court held Internet users to a higher level of sophistication, believing that users are responsible for having some background knowledge and mastery of internet technologies. Second, it is a common practice in the Internet industry to put hyperlinks of company policies such as “Baidu read before use” at the bottom of webpages. Although the hyperlink “Baidu read before use” is in small size, since the design of the webpage is quite simple with only limited pictures and texts, Internet users can find this hyperlink with an ordinary duty of care. Finally, in light of Information Security Technology — Guidelines for Personal Information Protection within Public and Commercial Services Information Systems, before dealing with personal information, OSPs need to receive permission from Internet users. The user can grant permission in an express or an
implied way, depending on the type of information being collected.\textsuperscript{67} When the OSP is collecting general personal information, it can be assumed to be permitted by users in an implied way, but if a user expressly objects to the collection of his general personal information, the OSPs need to stop collecting and deleting this information.\textsuperscript{68} However, when the OSP is collecting sensitive personal information, OSPs are required to get express permission from users.\textsuperscript{69} In this case, when collecting and utilizing the users’ anonymous information, Baidu adopts a policy of “express notification” and “implied permission”, which does not violate the public policy in respect to personal information protection in the Internet industry. Therefore, Baidu does not infringe the users’ right to know and choose.

2.1.5. Conclusion

The key underlying issue in \textit{Baidu v. Zhu Ye} was to reconcile the conflict between protecting privacy and promoting Internet industry. As stated in the decision by the Court of second instance, when deciding whether Baidu infringed the users’ privacy, the court ought to take into account the relationship between the protection of civil rights and the freedom of using information, and make sure that their decision echoes the needs of regulating order on the Internet while protecting the development of the Internet industry. In balancing these competing concerns, the court of the first instance favored privacy protection, whereas the court of the second instance gave preference to the Internet industry. Since this is the only case about cookie tracking so far, it is still too early to draw any definitive conclusions about the Chinese courts’ attitudes towards cookie tracking.

2.2: Secondary Liability

In the Internet era, many people participate in online social events on social network platforms run by online intermediaries. Some of these online social activities, such as expressing oneself via posts, contain potentially infringing information. Online intermediaries are held responsible for infringement occurring within their platform if they were found to have failed in their duty of care. Failure to meet this duty of care can subject online intermediaries to secondary liability.

In order to better clarify when OSPs may be held liable for privacy infringement committed by their users, this section divides secondary liability cases into two parts: cases in

\textsuperscript{67} Xinxi Anquan Jishu Gonggong Ji Shangyong Fuwu Xinxi Xitong Geren Xinxi Baohu Zhinan (信息安全技术公共及商用服务信息系统个人信息保护指南) [Information Security Technology — Guidelines for Personal Information Protection within Public and Commercial Services Information Systems], Article 5.2.3.

\textsuperscript{68} Id.

\textsuperscript{69} Id.
which OSPs were held liable and those in which OSPs were not. Accordingly, in analyzing each case under different subsections, the facts, court decisions, and comments are elaborated in turn.

### 2.1.1. OSP Held Not Liable Cases:


**Facts:**

This is a case concerns an article, which was published by the plaintiff’s deceased wife on a famous website in China called Tianya.cn (hereinafter Tianya) that accused him of cheating. Tianya has around 20 million registered users, and has established community rules, including the “Basic Rules of the Tianya Community” and “Website Keyword Filtering Measures”, which contain four levels of monitoring and filtering. The article at issue in this case contained the actual information of the plaintiff’s name and address. The plaintiff requested Tianya.cn to cease the infringing act, delete the related information on its website, apologize, and pay for the damages.

**Decision:**

The court concluded that, according to Article 13 of the Regulation on Internet Information Service of the People’s Republic of China,\(^{70}\) and Article 9 (8) of the Management Provisions on Electronic Bulletin Services in Internet,\(^{71}\) Tianya (as the manager of Tianya.cn) was responsible for monitoring\(^{72}\) the articles and posts which were published on its site. However,

---


\(^{72}\) The “monitoring” here is literally translated from “JianGuan (监管)” in the case decision. In light of the case decision, the monitoring obligation does not require OSPs to actively seek infringing materials but rather remove infringing materials after knowing them. In following text, the terminology “monitor” is also used in this sense.
the court determined that Tianya satisfied this monitoring requirement by establishing and
enforcing its community rules. The court considered the diversity of language used on the site
and recognized the reality that it is impossible for service providers to censor all the
responses of its users in advance of publication. The court indicated that the service provider’s
duty to monitor content is based on the prerequisite that it has actual knowledge that the
alleged information is infringing or illegal. If the service provider has actual knowledge of
the infringing nature of the content and chose to connive with the infringer’s distribution of
the infringing information, it is liable for the damages resulting from the infringement. If the
service provider did not have knowledge of the infringing content or if the service provider
promptly removed the information when it gained such knowledge, it will not be held liable
for infringement. Thus the court held that Tianya’s duty to monitor was limited to deleting or
modifying the allegedly infringing information when notified. Since Tianya removed the
article and related responses before the litigation and the plaintiff could not sufficiently prove
that he had ever raised complaints to Tianya, Tianya fulfilled its obligation and therefore was
not liable.

Comments:

It is obvious from the reasoning in this case that the court does not believe it is
possible for service providers to check every post being posted on their sites for potential
infringement, as the number is too big for a service provider to handle. Therefore, as long as a
service provider has established its own community rules and information filtering and
monitoring mechanisms, they are not liable for those slipped through that net. They are only
liable, when they have actual knowledge of the existence of the infringing items in their site
and fail to take corrective action. Since OSPs are not capable of examining the huge amount
of information on their websites, whether service providers have “actual knowledge” of the
infringing content mainly depends on whether the service providers have been notified by the
infringed party. Thus it will be safe for service providers to establish community rules and
promptly remove the alleged infringing items when notified by a third party.

(2) Xiang Li Yu Beijing Weimeng Chuangke Wangluo Jishu Youxian Gongsi Deng
Mingyuquan Jiufen An (向莉与北京微梦创科网络技术有限公司等名誉权纠纷案)
[Xiang Li v. Weibo.com], (First Interm. People’s Ct. of Beijing, Yizhongminzhongzi No.

73 Administration Procedures of Internet Information Services, art. 13; Management Provisions on Electronic Bulletin
Services in Internet, art. 9(8).
Facts:

The plaintiff registered several accounts in Weibo.com, a twitter-like social network platform. Several users on that platform posted multiple blogs which insulted and slandered the plaintiff, and revealed the plaintiff’s personal information. The plaintiff claimed that she sent complaints to Weibo.com and kept evidence (photocopies) of the complaints, but the service provider had not taken action against these blogs. The plaintiff therefore requested Weibo.com to cease its infringing activities and delete the infringing information on its site.

Decision:

The court first indicated that the blogs infringed the plaintiff’s reputation, and the plaintiff did provide photocopies of the correspondence to prove that Weibo.com had successfully received the plaintiff’s complaint. However, according to the Civil Procedure Law of China, 74 the Some Provisions of the Supreme People’s Court on Evidence in Civil Procedures, 75 and the then valid Opinions of the Supreme People’s Court on Some Issues Concerning the Application of the Civil Procedure Law of the People’s Republic of China, 76 considering the plaintiff failed to provide the original copies, the fact that the infringing blogs

74 Zhonghua Renmin Gonghe Guo Minshi Susong Fa (中华人民共和国民事诉讼法) [Civil Procedure Law of the People’s Republic of China] (Adopted at the 4th Session of the Seventh National People’s Congress on April 9, 1991; amended for the first time at the 30th Session of the Standing Committee of the Tenth National People’s Congress on October 28, 2007; and amended for the second time in accordance with the Decision on Amending the Civil Procedure Law of the People’s Republic of China as adopted at the 28th Session of the Standing Committee of the Eleventh National People’s Congress on August 31, 2012) art. 64.


had little influence as it is not prominently displayed on its site, and Weibo.com had removed
the infringing items after receiving the litigation documents, the court found Weibo.com not
liable.

Comments:

This case shows that, in order to demonstrate that the service provider was duly notified,
the plaintiff must make sure that all of the supporting evidence is original documents, hence
photocopies are not sufficient. However, as the 2015 Interpretation of the Supreme People’s
Court on the Application of the Civil Procedure Law of the People’s Republic of China has
already repealed the Opinions of the Supreme People’s Court on Some Issues Concerning the
Application of the Civil Procedure Law of the People’s Republic of China, according to its
Article 111, failing to provide original copy of the supporting evidence will not
automatically result in adverse consequences. Also, according to Article 5 of the Provisions
on Online Infringement of Personal Rights, a valid notice recognized by the people’s court
shall be “in writing or in the manner announced by the NSP”, and containing “(1) The name
and contact information of the informant; (2) The network address against which necessary
measures shall be taken as required or the relevant information sufficient to correctly locate
the infringing information; (3) the reason the informant demands deletion of corresponding
information.” And it is clearly indicated that the court will not support notices which do not
meet the criteria. In other words, the timing of the removal will be expanded from shortly

---

77 Zuigao Renmin Fayuan Guanyu Shiyong Zhonghua Renmin Gonghe Guo Minshi Susong Fa De Jieshi (最高人民法院关于适用《中华人民共和国民事诉讼法》的解释) [Interpretation of the Supreme People's Court on the Application of the Civil Procedure Law of the People's Republic of China] (Adopted at the 1636th meeting of the Judicial Committee of the Supreme People's Court on December 18, 2014, Interpretation No. 5 [2015] of the Supreme People’s Court) art. 111 (China), translated at LAWINFOCHINA, http://lawinfochina.com/Display.aspx?lib=law&Cgid=242703 (“Where it is indeed difficult to provide the original copy of documentary evidence as set forth in Article 70 of the Civil Procedure Law, including the following circumstances: (1) The original copy of documentary evidence is lost, extinguished or damaged. (2) The original copy, under control of the opposite party, is refused to be submitted despite lawful notification of submission. (3) The original copy is under the control of another person who is entitled not to submit it. (4) It is inconvenient to submit the original copy because of excess space or volume. (5) A party who bears the burden of proof is unable to obtain the original copy of documentary evidence through applying for investigation and collection by a people's court or other ways. Under the aforesaid circumstances, a people’s court shall review to determine whether the duplicate of the documentary evidence is able to be regarded as the basis for deciding the facts of a case, in combination with other evidence and the specific circumstances of the case.”).

78 Zuigao Renmin Fayuan Guanyu Shenli Liyong Xinxi Wangluo Qinhai Renshen Quanyi Minshi Jiufen Anjian Shiyong Falu Ruogan Wenti de Guiding (最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定) [Provisions of the Supreme People's Court on Several Issues concerning the Application of Law in the Trial of Cases involving Civil Disputes over Infringements upon Personal Rights and Interests through Information Networks] (promulgated by the Supreme People’s Court, FS[2014] No.11, Aug. 21, 2014) art. 5(China), translated at LAWINFOCHINA, http://lawinfochina.com/display.aspx?id=17960&lib=law (“Where, in accordance with paragraph 2, Article 36 of the Tort Law, the notice sent to a NSP by the infringed party in writing or in the manner announced by the NSP contains the following contents, the people’s court shall determine such a notice as valid: (1) The name (title) and contact information of the informant; (2) The network address against which necessary measures shall be taken as required or the relevant information sufficient enough to determine the infringement; (3) the reason the informant demands deletion of corresponding information. Where notices sent by persons suffering infringement do not meet the above criteria, and the network service provider holds they are exempt from responsibility, the People’s Court shall support this.”)
after notification by the plaintiff to the beginning of a subsequent lawsuit if the notification sent by the plaintiff is deemed insufficient.

(3) She Yong Su Hainan Tianya Zaixian Wangluo Keji Gufen Youxian Gongsi Sichuan Mala Wenhua Chuanmei Youxian Zeren Gongsi Qinfan Mingyuquan An (佘勇诉海南天涯在线网络科技股份有限公司、四川麻辣文化传媒有限责任公司侵犯名誉权案) [She Yong v. Tianya.cn and Sichuan Mala Culture & Media Co., Ltd.], (People’s Ct. of Chengdu Hi-Tech Industrial Development Zone, Gaoxinminchuzi No.2562, Nov. 24, 2014) (成都高新技术产业开发区人民法院 (2014) 高新民初字第 2562 号) (China).

Facts:

The plaintiff was a shareholder of a company which went into liquidation. Several posts appeared on Tianya.cn and Mala forum, which accused the plaintiff of embezzlement and causing the failure of the company. The plaintiff sued Tianya.cn and Mala forum for infringement of rights of reputation.

Decision:

The court first determined that the posts were infringing. It further pointed out that, according to Article 36 of the Tort Law of China, as Internet service providers, Tianya.cn and Mala forum are liable for infringement if they failed to undertake necessary corrective measures in a timely manner after they were notified of the infringement. Further, in accordance with Article 5 of the Provisions on Online Infringement of Personal Rights, the request sent by the plaintiff to Tianya.cn was deemed a sufficient notification. However, because Tianya.cn duly removed the infringing items after being notified by the plaintiff, Tianya.cn fulfilled its duty to monitor. The court also held that, according to Article 2 of the Some Provisions of the Supreme People’s Court on Evidence in Civil Procedures, since the

---

79 Tort Law of China, supra note 3, Article 36 ( “A network user or network service provider who infringes upon the civil right or interest of another person through network shall assume the tort liability. Where a network user commits a tort through the network services, the victim of the tort shall be entitled to notify the network service provider to take such necessary measures as deletion, block or disconnection. If, after being notified, the network service provider fails to take necessary measures in a timely manner, it shall be jointly and severally liable for any additional harm with the network user. Where a network service provider knows that a network user is infringing upon a civil right or interest of another person through its network services, and fails to take necessary measures, it shall be jointly and severally liable for any additional harm with the network user.”).

80 Zuigao Renmin Fayuan Guanyu Minshi Susong Zhengjiu De Ruogan Guiding (最高人民法院关于民事诉讼证据的若干规定) [Some Provisions of the Supreme People’s Court on Evidence in Civil Procedures] (promulgated by the Supreme People’s Court, FS[2001] No.33, Dec. 21, 2001, amended Dec. 31, 2008) art. 2(China), translated at LAWINFOCHINA, http://www.lawinfochina.com/display.aspx?lib=law&id=2197&C_gid= (“The parties concerned shall be responsible for producing evidences to prove the facts on which their own allegations are based or the facts on which the allegations of the
plaintiff could not provide evidence to prove that he sent take down notices to Mala forum and the latter failed to respond promptly, the fact that Mala forum has taken down the infringing articles after the litigation documents were served is sufficient to prove that Mala forum has fulfilled its duty to monitor.

Comments:

According to this case, the burden of proof is on the plaintiff to establish that he/she has already sent the notice to the service provider, and that the notice complies with the formal requirements of Article 5 of the Provisions on Online Infringement of Personal Rights. Failing to provide evidence of a competent take down request, or failing to prove that the request was received by the service provider (who took no corrective action), will result in the dismissal of a plaintiff’s infringement claim. From the perspective of a service provider, the provider should establish internal protocol for collecting and monitoring take-down notices and respond promptly to take down notices that comply with the statutory requirements. It is not necessary to respond to insufficient notices, as first, it is uneconomical to handle every claim; second, the information required is crucial for the provider to locate the alleged infringing action and determine whether the claim is reasonable or not.

2.2.2. OSP Held Liable Cases:


Facts:

The plaintiff is a famous professor from Tsinghua University and a member of the the Chinese People’s Political Consultative Conference (CPPCC) National Committee. The plaintiff published a holiday reform proposal during the annual sessions of the CPPCC, which suggested that the May Day Golden Week holidays should be cancelled. This proposal

81 This is a typical case reported by the Supreme People’s Court in chinacourt.org. See http://www.chinacourt.org/article/detail/2014/10/id/1456160.shtml (last visited, Aug. 11, 2015)
was subsequently attacked by netizens. Many Baidu Tieba users of Baidu.com created a BBS forum using the plaintiff’s name and posted several insulting articles containing the plaintiff’s personal information such as cellphone and home number. Baidu has established policies regarding the content posted by users and filing complaints. The plaintiff did not follow the set procedures for filing complaints, instead he entrusted one friend to call Baidu via phone, and send messages to the managing group of the BBS, but these complaints were ignored until Baidu received the cease and desist letter from the plaintiff. The plaintiff sued for cease infringement and the deletion of the BBS forum using his name.

**Decision:**

According to the court of first instance, the law does not require service providers to censor each and every post within their platforms. Service providers only have to notify users about their code of conduct, offer their users a channel to raise complaints, monitor content posted on their platforms, and remove inappropriate contents when necessary after receiving take down notices from the infringed party. Considering the fact that the service provider in this case, Baidu, had offered users a channel to raise complaints and had deleted the infringing items after receiving the cease and desist letter, Baidu was not liable for the infringement. The court denied the plaintiff’s request to delete the BBS forum using his name because the plaintiff is a public figure and the public is allowed to express their views on such figures, as long as they are not insulting. The BBS forum using the plaintiff’s name was simply a channel for the public to voice their opinion on the public figure, but there was no intention to infringe the plaintiff’s right to name.

However, the court of the second instance reversed, holding that Baidu was liable. The court indicated that Baidu have received the plaintiff’s complaint but only took action after receiving the cease and desist letter, thus Baidu was responsible for the damages happened after the receipt of the complaint. The court awarded damages for the plaintiff totaling 100 thousand yuan (approximately 15,400 USDs).

**Comments:**

This case illustrates the courts’ different attitudes towards the duty of care. The court of first instance found Baidu not liable, finding the fact that the plaintiff was a public figure dispositive. The court determined that in instances of infringement involving public figures, it

---

82 Baidu Tieba is an online community bound tightly with internet search services, one of the main business of Baidu. The website functions by having users search or create a bar (Forum) by typing a keyword, and if the bar has not been created before, it is then created upon the search. https://en.wikipedia.org/wiki/Baidu_Tieba
was unfair to hold Baidu to the same standard of care as cases involving members of the general public. The court of second instance found Baidu liable, basing its decision on the fact that the plaintiff sufficiently informed Baidu via public announced channels such as phone and messages in filing his compliant. That is to say, the court believed that, as long as the infringed party has notified the service provider via public announced channels, the service provider should take necessary measures accordingly. Moreover, the fact that an infringement was conducted on a service provider’s platform cannot sufficiently prove that the service provider knew its existence. Lastly, in handling cases involving public figures, the court tends to put more focus on the delicate balance between the freedom of expression and infringement. That is to say, for public figures, criticism is assumed. For posts related to them, so long as the post does not aim to insult them personally, it is allowed.

In this 2011 case, the court of second instance admitted that the official channels of complaint set by the service providers are critical in determining whether the plaintiff has sufficiently notified the service provider. However, it also noted that, the plaintiff can still rely on other channels, but the burden of proving notice is on the plaintiff. Three years after, in 2014, the Provisions on Online Infringement of Personal Rights was promulgated. Article 5 clearly provides that, a valid notice recognized by the people’s court should be “in writing or in the manner announced by the NSP”.

(2) Gong Weiwei Yu Beijing Tianying Jiuzhou Wangluo Jishu Youxian Gongsi Mingyuquan Jiufen An (龚蔚蔚与北京天盈九州网络技术有限公司名誉权纠纷案) [Gong Weiwei v. iFeng.com], (First Interm. People’s Ct. of Shanghai, Huyizhongminyizhongzi No. 1932, Sep. 28, 2014) (上海一中院（2014）沪一中民一（民）终字第1932号) (China).

Facts:

The plaintiff is a woman who had been sexually harassed in the subway. A video of the harassment was recorded and uploaded to iFeng.com afterwards by another passenger. The video was in high definition and uncensored, and the plaintiff’s friends could easily identify her in the video. The plaintiff responded in the comment block of the video page, through iFeng.com’s feedback page, and by calling iFeng.com’s customer service number, asking the defendant to delete the video or at least blur the plaintiff’s face. But iFeng.com only deleted the video after receiving the letter from the plaintiff’s lawyer, after the video had gained 1.4 million views.
Decision:

The court of the first instance first indicated that, considering the high number of views of the video and the fact that it was not removed promptly as the plaintiff requested, the video damaged the plaintiff’s reputation and iFeng.com was liable for infringement. The court further determined that, although the defendant argued that it was aware of the video only after receiving the letter from the plaintiff’s lawyer, the defendant was liable because the video had been widely reported by other media, and some of them even indicated that the video was from the defendant’s website. Therefore, iFeng.com ought to have known the existence of the video. The court thereby awarded damages for the plaintiff totaling 20 thousand Yuan (approximately 30,880 USDs), along with the compensation of the plaintiff’s attorney fee 3,000 Yuan (approximately 463 USDs), notary fee 1,500 Yuan (approximately 23 USDs), and case acceptance fee 1,332 Yuan (approximately 205 USDs).

The court of the second instance concluded that, the relationship between Paragraph 2 and 3 of Article 36 of the Tort Law of China is not progressive but parallel.\(^\text{83}\) That is to say, Paragraph 2 indicates that the plaintiff should notify the service provider if he/she found a third party committed a tort, but according to Paragraph 3, if the plaintiff can prove that the service provider knew the infringing activity, the plaintiff can demand the latter be liable for tort directly, without sending the take down notice in advance.

Comments:

This case clearly demonstrates that if an infringing party can prove that a service provider knows of the infringing activity, then the Paragraph 3 of Article 36 of the Tort Law of China applies and a take down notice is not necessary. According to the Article 9 of the Provisions on Online Infringement of Personal Rights, the following factors should be considered by courts when determining whether a service provider “knew” the infringing activity: (1) whether, either automatically or manually, the OSPs suggested, listed, selected, edited, organized, revised, or handled the infringing information in other ways; (2) the characters of service offered by OSPs, the ways of offering service, the possibility of leading to infringements through its service, and OSP’s capability of managing information; (3) what

\[^{83}\text{Tort Law of China, supra note 3, Article 36 (“A network user or network service provider who infringes upon the civil right or interest of another person through network shall assume the tort liability. Where a network user commits a tort through the network services, the victim of the tort shall be entitled to notify the network service provider to take such necessary measures as deletion, block or disconnection. If, after being notified, the network service provider fails to take necessary measures in a timely manner, it shall be jointly and severally liable for any additional harm with the network user. Where a network service provider knows that a network user is infringing upon a civil right or interest of another person through its network services, and fails to take necessary measures, it shall be jointly and severally liable for any additional harm with the network user.”).}\]
kind of personal right is infringed, and whether the infringement is obvious or not; (4) the information's impact on society and the viewing number in certain period; (5) the technical possibility allowing for OSPs to take measures against infringement, and whether the OSPs adopt reasonable measures to prevent infringements; (6) whether the OSPs take reasonable measures against repeat infringements committed by the same internet user or against the same infringing information; (7) other factors which need to be considered. In this case, the allegedly infringing information was viewed by a large number of internet users and reported extensively by the media, so the fourth factor weighed heavily in the plaintiff’s favor. The court found the strength of this factor sufficient to establish infringement. However, the court did not consider the other factors in detail, so it is unclear how these factors would be weighed by the courts.

Facts:

The defendant, Beijing Thousand Oaks Internet Technology Development Co., Ltd. (hereinafter Thousand Oaks), runs a social network platform in which the plaintiff was a registered user. The plaintiff found that another user had intentionally uploaded a number of uglified photos of her and posted several insulting articles to the platform, spreading them among the plaintiff’s social media connections. The plaintiff made several complaints to Thousand Oaks, but Thousand Oaks only deleted the photos, leaving the insulting articles. After receiving a court summons, Thousand Oaks blocked the alleged user. The plaintiff then sued Thousand Oaks for failing to fulfill its duty to monitor.

Decision:

The court of first instance ruled that, since all users of Thousand Oaks’ social network platform agreed to its User Regulation which prohibit the posting of infringing information, and Thousand Oaks as a service provider cannot censor each and every message posted on

---

84 Provisions on Online Infringement of Personal Rights, supra note 27, Article 9.
their site, the facts that it had removed infringing photos after being notified by the plaintiff, and that it had eventually deleted the alleged user account was enough to demonstrate that Thousand Oaks has fulfilled its duty to monitor. The court of the first instance also found that, since the evidence provided by the plaintiff were not sufficient to prove that she had contacted Thousand Oaks several times and the latter refused to delete the infringing items, Thousand Oaks was not liable for the infringement and the damage request could not be granted.

The First Intermediate Court reversed, claiming that the evidence provided by the plaintiff, snapshots of webpages that contain the complaints, was sufficient to establish infringement. According to Article 36 of the Tort Law of China, when information posted by a user is obviously infringing, the plaintiff has the right to notify the service provider and the latter should take necessary corrective measures. According to the correspondence evidence provided by the plaintiff, after being notified by the plaintiff, Thousand Oaks only deleted the related photos but failed to block the alleged infringing account, which allowed the tortfeasor to upload the infringing information again. This was sufficient evidence to prove that the corrective measures taken by the service provider were insufficient, and therefore the service provider was responsible for the aggravation of the damage. The court thereby awarded damages for the plaintiff totaling 30,000 Yuan (approximately 4,632 USDs), along with the notary fee 1,000 Yuan (approximately 154 USDs), and case acceptance fee 525 Yuan (approximately 80 USDs).

Comments:

This case involved two important issues: counterevidence required of the service provider and necessary corrective measures taken by the service provider. The intermediate court has made clear that, first, once the plaintiff introduces evidence of infringement, the service provider’s failure to provide counterevidence will leave the service provider at a disadvantage, as the court believes the latter is in a dominant position compared with users. Second, the “necessary measures” to correct infringement requires the service provider to take extensive measures necessary to stop the infringing actions. In this case, deleting the infringing items was not enough. Block the infringing account was the only way to stop the infringing activities.

(4) Li Ganghong Wang Guanling Su Hainan Tianya Zaixian Wangluo Keji Youxian Gongsi

Facts:

The plaintiffs’ relative was killed in a traffic accident, in which the driver was deemed to be fully responsible. One of the plaintiffs was a police officer, and several posts appeared on Tianya.cn accusing the plaintiff officer of extortion and calling him “a rascal.” The plaintiffs sent a take down notice to Tianya.cn on October 14, 2014, but the defendant considered the posts as a form of free expression thus took no action against them. The plaintiffs then sued Tianya.cn for failing to fulfill its duty to monitor, thereby violating their privacy and encroaching upon their right of reputation. The defendant subsequently deleted the posts after receiving litigation documents on November 18, 2014.

Decision:

The district court indicated that the posts on Tianya.cn contained content that clearly insulted and defamed the plaintiffs and damaged their reputations. The court determined that the defendant did not promptly react based on Article 6 of the Provisions on Online Infringement of Personal Rights. According to Article 36 of the Tort Law of China, because the plaintiffs sent a take down notice to the defendant via email and the defendant did not promptly react and take necessary measures to prevent the damage from growing, the court concluded that the defendant’s lack of action constituted infringement. However, the court did not support the privacy violation claim of the plaintiff, based on Article 12 of the Provisions on Online Infringement of Personal Rights. The court thereby awarded damages

---

85 Provisions on Online Infringement of Personal Rights, supra note 27, Article 6 (“When the People’s Court applies the provisions of Paragraph 2 of Article 36 of the Tort Law, to determine whether deletion, blocking, severance of links and other such necessary measures adopted by network service providers are timely or not, it shall judge the matter comprehensively on the basis of factors such as the nature of the network service, the form of valid notification and its degree of accuracy, the type and extent of the infringement of rights and interests through online information, etc.”).

86 Provisions of the Supreme People’s Court on Several Issues concerning the Application of Law in the Trial of Cases involving Civil Disputes over Infringements upon Personal Rights and Interests through Information Networks, Article 12 (“Where network users of network service providers use the network to publicize genetic information, medical history materials, health inspection materials, criminal records, household addresses, private activities and other personal information or personal privacy of natural persons, resulting in harm to the other person, and the person suffering infringement demands they bear tort liability, the People’s Court shall support this. Except under the following circumstances:
(1) the natural person has agreed in writing and publication takes place within the scope of the agreements;
(2) in order to spur the social public interest, and it is within the scope of necessity;
for the plaintiff totaling 1,500 Yuan (approximately 231 USDs), along with the attorney fee 3,000 Yuan (approximately 463 USDs), and case acceptance fee 44 Yuan (approximately 6 USDs).

Comments:

This case reveals two important considerations of the court: the promptness of the service providers corrective action and the availability of information elsewhere. First, the court has flexibility to determine whether a service provider’s response is prompt or not. Therefore, service providers should act as quickly as possible when they received notices from private parties and find that the items contain potential threats to one’s reputation or privacy. Second, as long as the private information can be acquired legitimately elsewhere (in this case are the name and affiliation of the plaintiff), there is no privacy invasion if that information is posted on service provider’s site. Besides disclosing “personal information that is already lawfully published”, the Article 12 of the Provisions on Online Infringement of Personal Rights also enumerates several other liability exemptions for privacy disclosure. However, regarding the other exemptions, no case decisions have indicated how courts will interpret them. Particularly, exemption 2 (disclosure for public interests) has not been defined, so it is still unclear how exactly these exemptions will be applied in judicial practices.

2.2.3. Compensation in the Case of Online Privacy Infringement

In China, there are explicit statutory provisions governing the calculation of compensation in cases involving the infringement of personal rights. According to Article 20 of the Tort Law of China, “Where any harm caused by a tort to a personal right or interest of another person gives rise to any loss to the property of the victim of the tort, the tortfeasor shall make compensation as per the loss sustained by the victim as the result of the tort. If the loss sustained by the victim is hard to be determined and the tortfeasor obtains any benefit

---

(3) by schools, scientific institutions, etc., for the purposes of scientific research for the public interest, or for statistical purposes, with the written agreement of the natural person, and the method of publication does not allow the identification of a specific natural person;
(4) where natural persons themselves publish this information online or other personal information that is already lawfully published;
(5) personal information that is obtained through lawful channels;
(6) except where laws or administrative regulations provide otherwise.
Where network users or network service providers publicize personal information as provided in Items 4 and 5 of the previous Paragraph in a manner that violates the social public interest or social morality, or the publication of the information concerned harms major interests of rights holders that merit protection, and the rights holder requests that network users or network service providers bear tort liability, the People’s Court shall support his.
Where State organs publish personal information in the exercise of their duties, the provisions of this Article do not apply.”.

87 Provisions on Online Infringement of Personal Rights, supra note 27, Article 12.
from the tort, the tortfeasor shall make compensation as per the benefit obtained by it. If the benefit obtained by the tortfeasor from the tort is hard to be determined, the victim and the tortfeasor disagree to the amount of compensation after consultation, and an action is brought to a people’s court, the people’s court shall determine the amount of compensation based on the actual situations.”88 Further, in light of Provisions on Online Infringement of Personal Rights, if both the loss sustained by the victim and the benefit obtained by the infringer are difficult to determine, the People’s Court shall determine the amount of compensation within 500,000 Yuan based on the actual situation.89

The infringer is also required to pay reasonable expenses that the victim spends for preventing infringement, including the costs of investigation and collecting evidence.90 In addition, based upon the victim’s request and the actual situations, the People’s court may decide that the compensation includes the attorney fees required for complying with the provisions stipulated by related authorities.91 In the following table, the compensation in the case of online privacy infringement is enumerated:

Table 1: compensation awarded by Chinese courts

<table>
<thead>
<tr>
<th>Case</th>
<th>Level</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cai Jiming v. Baidu.com</td>
<td>Second instance</td>
<td>Damage 100,000 Yuan</td>
</tr>
<tr>
<td>Gong Weiwei v. iFeng.com</td>
<td>First instance</td>
<td>Damage 20,000 Yuan, attorney fee 3,000 Yuan, notary fee 1,500 Yuan, and case acceptance fee 1,332 Yuan.</td>
</tr>
<tr>
<td>Wang Fang v. Beijing Thousand Oaks Internet Technology Development Co., Ltd.</td>
<td>Second instance</td>
<td>Damages 30,000 Yuan, along with the notary fee 1,000 Yuan, and case acceptance fee 525 Yuan.</td>
</tr>
<tr>
<td>Li Ganghong, Wang</td>
<td>First instance</td>
<td>Damages 1,500 Yuan</td>
</tr>
</tbody>
</table>

88 Tort Law of China, supra note 3, Article 24.
89 Provisions on Online Infringement of Personal Rights, supra note 27, Article 18.
90 Id.
91 Id.
The above cases demonstrate clear interpretive patterns of the Chinese courts in handling secondary liability cases related to the tort of infringing personal online information. Although the 2009 passage of the new Tort Law of China changed the underlying laws, these changes do not appear to significantly change the underlying judicial inquiries. First, as a basic principle, service providers should react promptly after they receive take down notices. Moreover, the service provider should take necessary corrective measures accordingly, as long as the infringed party has notified the service provider via the channel provided by the provider. However, service providers are only liable when they have actual knowledge of the existence of the infringing items on their site and take no action. Second, the service providers should also distinguish free expression from infringement. As long as the contents are unbiased and do not target a specific individual or public figure, the service providers should have more confidence in keeping the alleged infringing information on their platforms. Third, an infringed party’s failure to raise a complaint in a form recognized by the law, or to provide legitimate evidence of the complaint will cause the plaintiff to lose the case. Fourth, if the infringed party can prove that a service provider knows of the infringing activity and took no action, then a take down notice is not necessary to hold the service provider liable. Fifth, “necessary measures” means corrective measures sufficient to stop the infringing activities. If measures were taken but the infringer can still perform infringing actions on the site, then the service providers will be held liable for the damages thereafter. Sixth, the damages awarded by the court range from 1,500 Yuan (approximately 231 USDs) to 100,000 Yuan (approximately 15,440 USDs). In cases involving public figures or courts in major cities, the amount of damages tends to be higher.

Nevertheless, since only a limited number of cases have addressed the issue of OSP’s liability for online privacy infringement, several important issues have not been reviewed in detail, including how to interpret the essential elements of a competent notice, how to define “delete in a timely manner”, who should be liable for wrongful deletion, and how

---

92 Provision on Online Infringement of Personal Rights, supra note 27, Article 5. The detailed contents of this Article can be found in Part I, Section 1.2 (1).
93 Id. Article 6. Detailed contents of this Article can still be found in Part I, Section 1.2 (1).
to interpret the defenses to a claim of infringement.\textsuperscript{95} Regarding how to interpret the essential elements in a competent notice, so far, there have been no cases in which the court denied the competence of the notice sent by the plaintiff. Therefore, it seems, in light of these decisions of Chinese courts, it is not hard for a victim to send a competent notice. Regarding how to define “delete in a timely manner”, there is only one case where the court held that correction was not in a timely manner. In this case, the defendant deleted the complained contents on the fourth day after receiving the notice.\textsuperscript{96} Because of the short period deemed insufficiently timely in this case, OSPs should have procedures in place to deal with notices almost immediately. Regarding who should be liable for wrongful deletion, although no case has dealt with this issue, in light of the Judicial Interpretation, the notifier who sends wrong notice ought to be liable for the damage resulted from wrong deletion, and the OSP should not be found liable if it follows the notice.\textsuperscript{97} As for how to interpret the defenses to a claim of infringement, in the case of online privacy infringement, this clause has not been reviewed by the Chinese courts. Therefore, in order to draw a full picture of OSPs’ liability for online privacy infringement in judicial practice, more case decisions are needed.

\textsuperscript{94} Id. Article 7, 8. Detailed contents of these two Articles can still be found in Part I, Section 1.2 (1).
\textsuperscript{95} Id. Article 12. Detailed contents of this Article can be found in note 85.
\textsuperscript{96} See supra Part II, Section 2.2.2. (4).
\textsuperscript{97} Provision on Online Infringement of Personal Rights, supra note 27, Article 7-8.
Part III Identity Disclosure

The Internet is characterized by anonymity, which means that Internet users can easily hide their identities on the Internet. If Internet users commit illegal acts on Internet, OSPs may be obligated to disclose these Internet users’ identities to hold them responsible for violating laws online. Nevertheless, identity information is protected as private information, so identity disclosure should be done with the due process prescribed by law. In China, the regulations governing the disclosure of Internet users’ identity are quite fragmented. In the field of infringing personal rights, according to the Provisions on Online Infringement of Personal rights, based on the plaintiff’s request and circumstances in the case, a People’s Court may order the OSP to submit sufficient information that can identify the Internet users suspected of infringement, such as their name, contacts, IP addresses, etc. In the copyright infringement field, there exist several rules about the disclosure of infringers’ identities online. According to the Article 13 of Regulations on the Protection of Right of Dissemination via Information Network (hereafter Internet Regulations), the administrative department of copyrights may, for the purpose of investigating infringements upon the right of dissemination via information network, require the relevant OSPs to provide information such as the names, contact information, and the web addresses of its service objects who are suspected of committing copyright infringement. Further, where any Internet service provider refuses or delays to provide such identity information the administrative department of copyright may give the provider a warning. In the event of serious circumstances, equipment, such as computers that provide the Internet service, may be confiscated. Further, relevant Judicial Interpretations issued by People’s Supreme Court grant copyright owners the right to request Internet users’ identity information in civil procedures. According to the Interpretation of the Supreme People's Court on Several Issues Concerning the Application of Law in the Trial of Cases Involving Copyright Disputes over Computer Network (Internet Copyright Interpretation (2006)), copyright owners can request the registration information of Internet users from hosting OSPs for the purpose of suing the Internet users for copyright infringement. If the hosting OSPs refuse to provide the

98 Provisions on Online Infringement of Personal Rights, supra note 27, Article 4.
99 According to the Article 10(12) of Copyright Law of the People’s Republic of China, the right of dissemination via information network means the right to make a work available to the public by wire or wireless means, through which the public may access the work at times and places of their respective choice.
100 Regulation on the Protection of the Right Dissemination via Information Network (信息网络传播权保护条例), Article 13.
101 Id. Article 25.
102 Id.
registration information requested without fair reasons, they may undertake corresponding liability.\textsuperscript{103} Interpreting this Article literally, copyright owners can request hosting OSPs to disclose the alleged infringing users’ identities even without applying for orders from the courts.

The following sections examine relevant judicial decisions that interpret Chinese laws governing identity disclosure in the areas of (3.1) personal rights infringement, (3.2) copyright infringement, and (3.3) trademark infringement.

3.1. Identity Disclosure in the Case of the Online Infringement of Personal Rights

As referenced above, the Provision on Infringing Rights of Person permits a court to order an OSP to disclose the identity information of an alleged infringer of personal rights if requested by the plaintiff. Nevertheless, in practice, some victims request the OSPs to disclose the alleged infringing users’ identity information without applying for orders from the courts. Facing such requests, are the OSPs obligated to disclose the identity information? Further, upon receiving orders from courts, to what extent should the OSPs disclose the identity information?

3.1.1. Disclosure requests from victims


Facts:

In this case, the defendant QianXiangWangJing ran a social networking service similar to Facebook which allowed Internet users to create personal profiles, add other users as “friends”, and post and exchange information. The plaintiff found that a user of defendant’s service had her photos uglified and then posted these photos on the defendant’s website. Therefore, the plaintiff contacted the defendant’s customer service, and requested the

\textsuperscript{103} Interpretation of the Supreme People's Court on Several Issues Concerning the Application of Law in the Trial of Cases Involving Copyright Disputes over Computer Network (2006 Amendment) (最高人民法院关于审理涉及计算机网络著作权纠纷案件适用法律若干问题的解释(2006修正)), Article 5.
defendant to take down the photos in question. Besides of takedown request, the plaintiff also requested that the defendant disclose all the information relevant to identify the alleged infringing user, including the location where he usually logged in his account, ID number, etc. Regarding the plaintiff’s disclosure request, the defendant replied as follows: the logging location and other identity information were part of the user’s privacy, so the plaintiff was not authorized to get this information, and the defendant would only disclose this information upon the request of the police department or an order from the court.

**Decision:**

In the decision, the court held the defendant liable because it failed to expeditiously take necessary measures to block or disconnect the infringing links after receiving the takedown notice. Based on the facts of the case, the identity information requested was not required to support a finding of infringement. While the court did not directly rule on the disclosure issue, it can be inferred that an OSP is not obligated to disclose an alleged infringing user’s identity information upon the request of a victim of the infringement.

**Comments:**

As a typical case decision reads, due to the anonymity afforded by the Internet, establishing the identity of infringing users is often a difficult element for plaintiffs to prove. The issue is further complicated by Internet companies’ obligation to keep Internet users’ identity confidential. In order to reconcile conflicts between privacy protection and the protection of other legal interests, any request of identity disclosure ought to be examined by courts before granting it, since judicial review can better reconcile the conflicts by balancing competing interests. Therefore, OSPs are only obligated to disclose the alleged infringing users’ identity information upon the orders from courts rather than the requests sent by victims.

### 3.1.2. The criteria of identity disclosure

---

104 The court decided this case by referring to the Article 36 of Tort Law which reads as follows: “where a network user commits a tort through the network services, the victim of the tort shall be entitled to notify the network service provider to take such necessary measures as deletion, block or disconnection; if, after being notified, the network service provider fails to take necessary measures in a timely manner, it shall be jointly and severally liable for any additional harm with the network user.”

105 These so-called typical cases are selected and published on the website “ChinaCourt”, so these typical cases have wide impact on the judicial practice in China.


107 *Id.*

108 *Id.*
Case citation: Zhao Xinqiang Yu Xianrenqiu Wenhua Chuanmie Youxian Gongsi Wangluo Qinquan Jiufen An (赵信强与仙人球文化传媒有限公司网络侵权纠纷案) [ZhaoXinQiang v. XianRenQiu Culture Media Inc.], (People’s Court of LeQing, Wenleminchuzi No. 159, March 26, 2015) (乐清市人民法院) (2015)温乐民初字第159号 (China).

Facts:
In this case, the defendant XianRenQiu ran a BBS that allowed its users to post information on it. The plaintiff found that a user called “GreenTea” posted three articles defaming him on the BBS, so he requested that the defendant not only block and disconnect the links to these three articles, but also disclose the IP addresses and identity information of the user “GreenTea”. Upon receiving the plaintiff’s request, the defendant deleted the defamatory articles, but did not provide the IP addresses and identity information of the user “GreenTea” to the plaintiff. Therefore, the plaintiff applied for a court order to disclose the following information: (1) the IP addresses used by “GreenTea” to post and reply the defamatory articles; (2) the registration information of “GreenTea” and its detailed identity information; (3) the viewing number and retransmission number of the three articles.

Decision:
In the decision, the court first confirmed that the plaintiff had right to know the identity information of “GreenTea”, since the articles posted by “GreenTea” were suspected of infringing the plaintiff’s personal interests. Then, the court further held that the defendant must disclose the identity information in the level of detail permitted by their technology. However, the court only confirmed the plaintiff’s second request and dismissed the other two. Therefore, the court set a restriction on an OSP’s obligation of identity disclosure, only requiring the service provider to disclose the identity information within the level of detail permitted by their Internet technologies.

Comments:
The breadth of required identity disclosure in this case is representative of typical judicial approaches to this issue. The court held that the defendant should disclose the two alleged infringing bloggers’ identity information within its capacity permitted by the Internet
technologies.  Since OSPs may not keep all the identity information that plaintiff’s request or may not keep enough information to identify infringers, case law in China only requires OSPs to disclose the identity information within its capacity permitted by the Internet technologies.

3.2. Identity Disclosure in the Case of the Online Infringement of Copyright

As referenced above, the Internet Copyright Interpretation (2006) provides that copyright owners can request hosting OSPs\(^{110}\) to disclose the alleged infringers’ identity information. In several cases, copyright owners have attempted to require Internet access providers and P2P websites to disclose infringing users’ identity information, but eventually failed.\(^{111}\) Because of its limited sphere of application, this identity disclosure clause has only been reviewed by Chinese courts in limited cases.

1. Case 1: Qiao Moumou Yu Beijing Tiexue Keji Youxian Gongsix Qinfan Zhuzuoquan Jiufen An (乔某某与北京铁血科技有限公司侵犯著作权纠纷案) [Qiao Moumou v. tiexue.net], (Haidian District Court of Beijing, Haiminchuzi No. 15359, July 19, 2006) (北京市海淀区人民法院（2006）海民初字第15350号) (China)

In this case, the defendant ran a website “tiexue.net” which allowed its users to upload pictures on it. The plaintiff Qiao found that some of his copyrighted pictures were uploaded to tiexue.net without permission, so Qiao sued the defendant for copyright infringement. The defendant did not submit the registration information of Internet users who uploaded the infringing pictures, so the court found this non-disclosure an important factor in finding the defendant liable for the copyright infringement.

2. Case 2: Qiao Moumou Yu Beijing Huawanghuitong Jishu Fuwu Youxian Gongsix Qinfan Zhuzuoquan Jiufen An (乔某某与北京华王惠通科技服务有限公司侵犯著作权纠纷案) [Qiao Moumou v. huawanghuitong.com], (Haidian District Court of Beijing, Haiminchuzi No. 15360, July 19, 2006) (北京市海淀区人民法院（2006）海民初字第15360号) (China)

In this case, the plaintiff attempted to require the defendant – a P2P website to disclose an infringing user’s identity, and the court held that the trial court decision could only be made to hosting OSPs rather than P2P websites. In the case of LiMou Su verycd.com, the plaintiff tried to request the defendant – a P2P website to disclose an infringing user’s identity, and the court held that the trial court decision could only be made to hosting OSPs rather than P2P websites. See Limou Su verycd Gongsi Qinhai Xinxide Shengzhi Wangluo Chuanboquan Jiufen An (李某诉verycd公司侵害信息网络传播权纠纷案) [LiMou v. verycd.com] (MinHang District Court, Minmiansanzhichuzi No. 175, Aug. 22, 2012) (闵行区人民法院), (2012) 闵民三(知)初字第175号 (China). In the case of ZheJiangDongYangTianShi Culture v. Baidu and China Telecom, the plaintiff got the IP address used for infringement, and then requested China Telecom – an Internet access provider to disclose the identity of the owner of the IP address, and the court held the disclosure request could only be made to hosting ISPs rather than Internet access providers. See Zhejiang Dongyang Tianshi Wenhua Chuanbo Youxian Gongsi Yu Beijing Baidu Wangxuan Keku Youxian Gongsi Deng Qinfan Zhuzuoquan Jiufen An (浙江东阳天世文化传播有限公司与北京百度网讯科技股份有限公司等侵犯著作权纠纷案) [ZheJiangDongYangTianShi Culture v. Baidu and China Telecom] (First People’s Intermediary Court of Beijing, Yizhongminzhongzi No. 2232, Mar. 29, 2013) (北京市第一中级人民法院, (2013)一中民终字第2232号) (China).

---


\(^{110}\) To be mentioned, in light of Internet Copyright Interpretation (2006), only hosting OSPs are obligated to disclose the alleged infringers’ identity upon copyright owners’ requests.

\(^{111}\) In the case of LiMou v. verycd.com, the plaintiff tried to request the defendant – a P2P website to disclose an infringing user’s identity, and the court held that the trial court decision could only be made to hosting OSPs rather than P2P websites. See Limou Su verycd Gongsi Qinhai Xinxide Shengzhi Wangluo Chuanboquan Jiufen An (李某诉verycd公司侵害信息网络传播权纠纷案) [LiMou v. verycd.com] (MinHang District Court, Minmiansanzhichuzi No. 175, Aug. 22, 2012) (闵行区人民法院), (2012) 闵民三(知)初字第175号 (China). In the case of ZheJiangDongYangTianShi Culture v. Baidu and China Telecom, the plaintiff got the IP address used for infringement, and then requested China Telecom – an Internet access provider to disclose the identity of the owner of the IP address, and the court held the disclosure request could only be made to hosting ISPs rather than Internet access providers. See Zhejiang Dongyang Tianshi Wenhua Chuanbo Youxian Gongsi Yu Beijing Baidu Wangxuan Keku Youxian Gongsi Deng Qinfan Zhuzuoquan Jiufen An (浙江东阳天世文化传播有限公司与北京百度网讯科技股份有限公司等侵犯著作权纠纷案) [ZheJiangDongYangTianShi Culture v. Baidu and China Telecom] (First People’s Intermediary Court of Beijing, Yizhongminzhongzi No. 2232, Mar. 29, 2013) (北京市第一中级人民法院, (2013)一中民终字第2232号) (China).
In this case, the same plaintiff Qiao sued the website china.com for copyright infringement based on facts similar to the previous case. During the hearing, the defendant submitted the registration information of Internet users who allegedly committed copyright infringement, and the court held that the defendant fulfilled its duty of disclosing the infringers’ identities. However, the registration information disclosed by the defendant only included the so-called internet names such as “wolf”, “keer” and “axjidy”, and associated e-mail addresses, which did not help the plaintiff identify the real infringers.


In this case, the plaintiff found a TV series copyrighted by it was uploaded to the defendant’s website by an Internet user named as “Mo Daqian (莫大千)”. In addition to suing the defendant for contributory infringement, the plaintiff also requested the defendant to disclose the Internet user Mo Daqian’s real name, address, phone number, email address and the IP address used for uploading the TV series. However, during the hearing, the defendant merely provided Mo Daqian’s registration information and IP address, which was not sufficient to identify Mo Daqian. Finally, the court held that the defendant had already fulfilled the obligation of identity disclosure based on the following reasons: (1) it was unreasonable to require the hosting OSPs to disclose more identity information than was provided by its users when registering the accounts; (2) the defendant had proved that the registration information disclosed by it was true. Therefore, since Internet users usually do not need to register accounts by submitting their real identity information, in most cases, the registration
information retained by hosting OSPs normally cannot reveal the real identities of Internet users.\textsuperscript{112}


Despite these challenges, it is still possible for copyright owners to receive sufficient identity information from hosting OSPs in some occasions. In the case of 3rd Mian Xiang v. Great Wall Broadband, the defendant Great Wall Broadband provided webhosting services, and the plaintiff\textsuperscript{113} found that some of its copyrighted books were unlawfully available on a website hosted by the defendant. The plaintiff sued Great Wall Broadband for copyright infringement. In this case, even before filing a lawsuit, the plaintiff sent the defendant a notice which requested the defendant to disclose the alleged infringer’s registration information. The defendant submitted the corresponding registration information to the plaintiff. The registration information included the client’s real name, personal ID number and even their address, which was enough for the plaintiff to identify the direct infringer. Based on the facts above, the court held that the defendant fulfilled its duty of disclosing identity information.

5. Comments:

From the case law discussed above, in copyright field, China has not established strict procedures for the disclosure of Internet users’ registration information. In the first three cases, the registration information in question was disclosed under the orders of the courts, but in the final case, the registration information was disclosed directly upon the request of the copyright owners without any review by the court. Since the registration information may

\textsuperscript{112} In the other two disputes between joy.cn and tudou.com, the defendant tudou.com even failed to disclose the alleged infringing users’ registration information because these information has been lost, and the courts still held tudou.com fulfilled its obligation of identity disclosure. See Shanghai Jidong Wangluo Youxian Gongsi Yu Shanghai Quantudou Kiji Youxian Gongsi Qinfan Zhuzuo Caichanquan Jiufen An (上海激动网络有限公司与上海全土豆网络科技有限公司侵犯著作权纠纷案) [joy.cn v. tudou.com] (First People’s Intermediary Court of Shanghai, Huyizhongminwuzhichuzi No. 53, April 20, 2009) (上海市第一中级人民法院, (2009)沪一中民五 (知) 终字第 53 号) (China); Shanghai Jidong Wangluo Youxian Gongsi Yu Shanghai Quantudou Kiji Youxian Gongsi Qinfan Zhuzuo Caichanquan Jiufen An (上海激动网络有限公司与上海全土豆网络科技有限公司侵犯著作权纠纷案) [joy.cn v. tudou.com] (First People’s Intermediary Court of Shanghai, Huyizhongminwuzhichuzi No. 102, Nov. 25, 2009) (上海市第一中级人民法院, (2009)沪一中民五 (知) 终字第 102 号) (China).

\textsuperscript{113} In this case, the plaintiff is a copyright agency company, and it got authorization to sue infringers from copyright owners whose books were unlawfully transmitted.
reveal the identities of Internet users, which should be protected as their private information, any request to disclose registration information is supposed to be reviewed by the court to prevent the abuse of this disclosing procedure. Regarding the extent of identity information that must be disclosed, the Chinese courts adopt criteria similar to those followed by the courts in the case of infringing the rights of persons. In copyright field, OSPs only need to disclose the identity information permitted by its Internet technologies, such as the users’ registration information. If an OSP can prove the Internet technologies do not allow it to retain users’ identity information, it does not need to disclose any identity information.

In the latest Judicial Interpretation on online copyright infringement, the clause concerning identity disclosure is repealed. Therefore, currently there is no specific provision governing identity disclosure in online copyright infringement cases. How does the absence of the identity disclosure clause impact judicial practice? Does it mean copyright owners cannot request hosting OSPs to disclose the alleged infringers’ identity in copyright case, or can copyright owners still make the requests? After the enactment of the latest Judicial Interpretation, no online copyright case has dealt with the request of disclosing the alleged infringers’ identity information. Hence, there are still no clear answers these questions.

3.3. Identity Disclosure in the Case of the Online Infringement of Trademarks

In China, online shopping is immensely popular among consumers, so auction platforms like Taobao (run by Alibaba Group) develop quite rapidly. Like many other auction platforms, many products sold on Taobao are suspected of trademark infringement. Since the sellers on Taobao usually do not reveal their real identities, trademark owners encounter difficulties when suing infringing sellers. Therefore, identity disclosure is necessary on auction platforms to enforce trademark rights. Nevertheless, so far, neither Trademark Law nor relevant Judicial Interpretations rule on the identity disclosure on auction platforms. In order to solve the trademark infringement disputes on it platform, Taobao has prescribed its own identity

---

114 Provisions on Several Issues Concerning Application of Law in Civil Dispute Cases of Infringing Right of Dissemination via Information Network (最高人民法院关于审理侵害信息网络传播权民事纠纷案件适用法律若干问题的规定), Judicial Interpretation 2012 No. 20, passed on Nov. 26th, 2012, the Trial Committee of Supreme People’s Court, Conference No. 1561. (法释〔2012〕20号, 2012年11月26日最高人民法院审判委员会第1561次会议通过). According to the last Article of this Judicial Interpretation, it replaces the Internet Copyright Interpretation (2006).

115 I searched on the website “Judicial Opinions of China” on which the judicial decisions are published, but have not found any case involving identity disclosure in the case of online copyright infringement after the enactment of the latest Judicial Interpretation. See http://www.court.gov.cn/zgcpwsw/, (last visited Aug. 6, 2015).

116 See Trademark Law of People’s Republic of China (中华人民共和国商标法); Interpretation of the Supreme People’s Court Concerning the Application of Laws in the Trial of Cases of Civil Disputes Arising from Trademarks (最高法关于审理商标民事纠纷案件适用法律若干问题的解释), FS[2002] No. 32 (法释[2002]32号). Neither of these two documents mentions about identity disclosure in trademark infringement cases.
disclosure rules. Because of Taobao’s dominated position in auction platform market, the rules prescribed by Taobao have become the de facto standard for identity disclosure on auction platforms in China. To receive the identity information of a suspected infringer, the trademark owner must send relevant documents to Taobao, who then decides whether to disclose the identity information after evaluating the documents offered by the trademark owners. Therefore, Taobao performs the role of a private judge in dealing with identity disclosures on its platform. Taobao’s rules seem to be recognized by Chinese courts. In the case of Guo Donglin v. Wu Yundi, when the plaintiff received the defendant Wu Yunti’s identity through Taobao’s identity disclosure mechanism, the court did not question the legality of the identity disclosure. In another trademark case, the court also confirmed the validity and legality of receiving the alleged infringer’s identity through the identity disclosure mechanism on Taobao.

In summary, due to the absence of legislation governing the field of online trademark infringement, the auction platform giant Taobao prescribes its own rules on identity disclosure. In light of these rules, the identity information of sellers suspected of trademark infringement can be disclosed to trademark owners without judicial review, and Taobao has discretion to decide whether to disclose the identity information of its users. Since Taobao has the only tiny interest in each seller on its auction platform, it tends to follow the trademark owners’ requests for identity disclosure to avoid being held jointly and severally liable.

Conclusion:

Regarding OSPs’ obligation of identity disclosure, the Chinese courts follow different rules in the field of personal rights, copyright, and trademark. In the field of personal rights, an OSP is only obligated to disclose the suspected infringer’s identity information upon the order from a court. However, in the field of copyright, an OSP can disclose the suspected infringer’s identity information upon the victim’s request without any review done by a court.

118 Id.
As for the online trademark infringement, there is no explicit provision governing identity disclosure, and the Chinese courts recognize the identity disclosure rules set by Taobao.com—the largest auction platform in China. Since Taobao.com keeps the real identity information of sellers on its platform, the information disclosed by Taobao.com can identify sellers suspected of trademark infringement. Nevertheless, in the cases of online infringement upon personal rights and copyright, the OSPs usually do not keep sufficient information to identify the suspected infringers, so the Chinese courts only require the OSPs to disclose the identity information allowed by Internet technologies.

Conclusion

In China, the rules on privacy protection are quite fragmented. Nevertheless, regarding OSP’s liability for privacy infringement, the governing rules are mainly provided in the Article 36 of Tort Law of China and the Provisions on Online Infringement of Personal Rights. In addition, the authorities in China have also promulgated several regulations to govern the OSP’s tracking, collecting, and utilizing of Internet users’ private information. Since the governing regulations normally only refer to “related authorities” when providing which legal authorities are responsible for enforcing privacy on Internet, OSPs may face unexpected investigations from the authorities which claim they are authorized to enforce Chinese privacy laws.

Based on the case study in Part II, there are a limited number of cases examining OSPs liability for privacy infringement claims. Further, the OSPs will not typically be liable for privacy infringement committed by their users if they remove the infringing information complained of in formal notices. In the cases where the OSPs have been held liable, the courts mainly justified their decisions on the following reasons: (1) failure to remove infringing information in a timely manner; (2) failure to sufficiently remove the infringing information; (3) failure to act when the OSP should have known of the infringement. Further, several important issues still have not been reviewed by Chinese courts in detail, including: how to interpret the essential elements of a competent notice, how to define “delete in a timely manner”, who should be liable for wrongful deletion, and how to interpret the defenses to a claim of infringement. In addition, concerning OSPs’ direct liability, so far, there is only one case dealing with cookies tracking, and the courts of first instance and second instance delivered opposite opinions.
Regarding OSPs’ obligation of identity disclosure, there is no unitary rule, and in light of case law, OSPs in China follows different rules in the field of personal rights, copyright and trademark. In the authors’ opinion, since identity disclosure conflicts with Internet users’ privacy, any disclosure request ought to be reviewed by the courts. Generally, in respect of identity disclosure, the Chinese courts have not imposed a high level of obligation on OSPs, since they only need to disclose the identity information allowed by Internet technologies.