On an internet service provider's content management obligation and criminal liability*

PhD TU Longke**

Abstract

The online content management is one of ISP's obligations of internet safety management. The ISP is not obliged to initiatively review and supervise the online content, but it shall perform the proactive obligations of report and deletion afterwards. Different ISPs' content management obligations and criminal liabilities are distinguished on basis of different types of content provided by ISPs. The Direct Control Theory shall be adopted to determine whether an ISP has the content management obligation and assumes criminal liability so as to reasonably delimit the scope of criminal liability and avoid the uncertainty and expanse of the subject of criminal liability.

Keywords*: Internet Service Provider (ISP), Content Management Obligation, Criminal Liability*

I. Introduction

At present, cyber illegalities and crimes are rampant with unceasingly-spread violent, terrorist and sexual information, frequently-found online gamble and fraud, and personal information protection existing in name only. In current situation of huge number, extensive hazards and low cost of cyber illegalities and crimes and being hard to investigate and punish them, it becomes a common choice of criminal policy worldwide to curb cybercrimes, protect internet safety and regulate internet order from the perspective of regulating ISPs who enjoy technological advantages and controlling position. However, due to insufficient elaboration of theoretical foundation of criminal punishment, unclear delimitation of boundary of liability, vague standards for determining liability, there always are unceasing theoretical debates and indecisive judgments along with every nation's efforts in imposing criminal liability on ISPs. In China, some influential cases such as QvodPlayer case and deep linking case arouse attention of the whole society. The struggled performance of prosecutors in trial, the unclear elaboration in judgments of courts, divergent theoretical explanations in academia and the public's burning satire and freezing irony towards the criminal involvement constitute the practical scenery of imposing criminal liability upon ISPs in current China. The judicial embarrassment reflects the tenuity of the theoretical establishment and serious insufficiency of the connectivity between theory and practice, which influences the realization of aim of legislations on internet order governance and national strategy on internet safety, even fundamentally erodes the authority of criminal justice and hinders the whole process of modern legal construction.

* This paper is sponsored by the Innovative Project of Criminal Science of Law of Shanghai Academy of Social Sciences.

** Professor of Institute of Law of Shanghai Academy of Social Sciences, PhD in Law, a visiting scholar of School of Law of Oklahoma City University.

E-mail:tulongke1981@126.com.

The newly-adopted Amendment IX to Criminal Law of China creates a new mode of ISP's[1] criminal liability, that is to say, an ISP who fails to perform its obligation of internet safety management, thus resulting in hazardous consequences such as causing illegal information widespread, will face criminal punishment. The scope of internet safety management obligations is extensive, one of which is the online content management obligation aiming at prevention of illegal information from spreading on the internet. Currently, the criminal law scholars' research into the ISP's content management obligation and criminal liability in China is insufficient. There is a need to deeply analyse several issues such as whether it is necessary to reasonably delimit the scope of the content management obligation, whether it is all online content providers or certain online content providers have the obligation of content management and assume criminal liability accordingly, what differences there are in conditions for assuming criminal liability for different ISPs.

II. One Precondition for Criminal Liability: The Scope of Online Content Management Obligation

The ISP's online content management obligation may be classified into three types according to the time when there occurs illegal information: the first one is the obligation to pre-review online content; the second one is the obligation to real-timely monitor online content; the third one is the obligation to report and delete illegal information after it appears on the internet. Regarding whether an ISP's obligation to manage the content generated by the third party on the online platform offered by itself is a precondition for the ISP to assume criminal liability for the consequence of wide spread of illegal information, there are a lot of disputes abroad and they have not been settled yet. The positive argument states that the risk of bringing about illegal or right-infringing information is a natural side-product of internet service, so the principle of a responsible enterprise requires the ISP to regard the loss arising from such risk as a kind of business operation cost. This will force the internet servicer to prevent illegal information from occurrence and allocate the loss arising from such risk among the group of internet users[2]. In addition, the internet servicer enjoys ownership over devices storing, manufacturing and transmitting illegal information and the servicer's control over the ownership is sufficient for the service to be responsible for the emergence and transmission of illegal information on the internet[3]. The negative argument states that firstly, the internet servicer is not responsible for its user's behaviour. The internet service does not necessarily result in the emergency of illegal or criminal behaviour. Secondly, the expanse of ISP's responsibility will possibly make it have strong motive to delete users' materials from the internet for protecting its economic interests even though there is no illegal information. Thirdly, this kind of indifferent review system contradicts the regulation on freedom of speech in the

[1] Although the Criminal Law of China doesn't clearly state the connotation and types of ISP, after research into criminal legislation of China the author find that an online content provider generating or uploading content online does not belong to the ISP because there is another route for criminally investigating and prosecuting the former. Therefore, in this paper, unless otherwise stated, an ISP does not include an online content provider.

[2] Alfred C. Yen (2000). *Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise Liability, and the First Amendment*, The Georgetown Law Journal, 88, 4.

[3] Alfred C. Yen, cited, p. 38-45.

Constitutional Law[4]. Finally, it needs a lot of human resources to review such huge documents and information uploaded to the internet, so the addition of such obligation will lead to failure to get access to the internet[5]. Although the debate is fervent and long-lasting, in view of the balance among citizens' freedom of speech, internet technology development and protection of the victim's rights, it is commonly believed that an ISP shall undertake online content management obligation within reasonable scope.

The key issue is how to delimit the reasonable scope of online content management obligation of an ISP. The legal practices in foreign countries mostly deny the ISP's obligation to pre-review and real-timely monitor the content expressed by others on the internet. In 2011, the Court of Justice of the European Union decided in the influential *case of Scarlet v. SABAM*[6] that internet service providers have no general obligation to filter or monitor illegal information transmitted online and made clear that any competent authority shall not require the ISP to install the contested filtering system. The reasons are as follows: at the time of imposing obligations on an ISP, regard shall paid to the balance against the protection of the fundamental rights of individuals and the protection of the freedom of the ISP concerned to conduct its business. On one hand, the requirement for an ISP to install the contested filtering system would result in a serious infringement of the freedom of the ISP concerned to conduct its business; on the other hand, it is unnecessarily complicated or costly from the cost-benefit perspective[7]. Based on these reasons, the Court of Justice of the European Union denied the ISP's obligation to review the content. In the USA, there is no legislation specially clarifying whether the ISP has general review and monitoring obligation. It is commonly believed that the legislative intention of the Parliament is obvious that ISP has no obligation to monitor the content expressed by any third party in its website[8]. In the specialized legislation field, the principle of the copyright owner assuming responsibility to search infringement of copyright and inform service providers set forth in the Digital Millennium Copyright Act releases the ISP from the monitoring obligation[9]. The next issue is whether an ISP has the management obligation to report or delete the illegal information that has appeared. It is generally believed that ISP has no general management obligation unless specially otherwise stated. In the precedents such as Zeran v. America Online, Inc[10] Doe v. MySpace[11] and other classic cases, ISPs uniformly cited Section 230[12] to claim immunity from responsibility. This is a non-responsibility clause in the Communications Decency Act (CDA) provides immunity from liability for

[4] Alfred C. Yen, cited, p. 33-37.

[5] Lawrence G. Walters (2012), *Shooting the Messenger: An Analysis of Theories of Criminal Liability Used Against Adult- Themed Online Service Providers*, in Stanford Law and Policy Review, 171, 10.

[6]Scarlet Extended SA v Société belge des auteurs compositeurs et éditeurs SCRL（EU: Case C-70/10 Celex No. 610CC0070）.

[7] *Case of Scarlet v. SABAM,* Court of Justice of the European Union, Judgment of the Court (Third Chamber), 24 November 2011, In Case C‑70/10.

[8] See *case Stoner v. eBay*, Inc., No. 30566, 2000 WL 1705637, at *3 (Cal. Sup. Ct., Nov. 1, 2000) („[M]any of these products may be contraband, and however many it might be possible for defendant to identify as such, Congress intended to remove any legal obligation of interactive computer service providers to attempt to identify or monitor the sale of such products."); 141 Cong. Rec. H8468-69 (daily ed. Aug. 4, 1995) (statement of Rep. Cox).

[9] See Robert A. Gorman, Jane C. Ginsburg, 2006. *Copyright: Cases and Materials,* 7th ed., Foundation Press.

[10]Case *Zeran v. America Online*, Inc., 129 F.3d 327 (4th Cir. 1997).

[11] *Case Doe v. MySpace*, Inc., 528 F.3d 413 (5th Cir. 2008).

[12] 47 U.S.C. §230

those servicerswho provide visiting access to information generated by any third party or users, thus essentially denying ISPs' content management obligation. However, in circumstances where the law specially states otherwise, for example in the case of intellectual property infringement, upon the valid notification by the property owner, the ISP shall fulfill its management obligation. For example, in the attention-arousing and disputable Digital Economy Act of UK, in case of Online infringement of copyright, an internet service provider must provide a copyright owner with a copyright infringement list for a period if the owner requests the list for that period and an initial obligations code requires the internet service provider to provide it. if necessary, an ISP shall adopt technical measures to limit some or all relevant users' internet access for preventing or reducing copyright infringement through internet[13].

There were doubts about the ISP's content management obligation in China in the course of drafting and deliberating the Amendment IX to Criminal Law. The main reasons were as follows: It's hard to define the ISP's content management obligation; An ISP hasn't enough time and resources to tell whether relevant information is illegal or not; The imposition of obligation to review appendixes may hinder the development of internet science and technology[14]. Investigating substantive laws, we find that Article 5 of Decision of the Standing Committee of People's Congress of PRC on Strengthening Internet Information Protection sets forth that ISPs shall strengthen the management of information published by their users, promptly stop transmitting information prohibited by a law or regulation from publishing or transmission if any being found, take countermeasures such as deletion, keep relevant records and send a report to the competent authority. The dominant view in China denies the ISP's content review obligation by citing this article with the reason that the precondition for an unit providing internet service to assume such obligation is any illegal information „being found", which obviously does not impose the obligation to proactively „find out"illegalities and hazardous information on such unit, but means that the unit shall undertake corresponding responsibility when someone tell it or there is proof showing that the unit is aware of the existence of relevant illegalities and hazardous information[15]. The ISP generally assumes no statutory obligation to proactively review or monitor information uploaded or transmitted by any third party, but passively delete or report it afterwards. However, there is also another understanding on this issue. Some courts hold that the ISP, compared with the copyright owner, is more able to control and reduce such infringement, so from the perspective of the balance between rights and obligations, abilities and responsibilities, it is fairer to impose the obligation of strictly reviewing the content transmitted by internet users upon the service provider[16].

This paper holds that it is not suitable to impose pre-review and real-time monitoring obligation upon the ISP because such imposition would inevitably result in too heavy burden on the ISP, harm the freedom of the ISP concerned to conduct its business and narrow its development space. With social development changing rapidly and new things emerging in an endless stream, the legal obligation will definitely often evolve and is updated. The scope of „illegal information" is so extensive, including various types of information violating a law or regulation such as violating an administrative law

---

[13] Digital Economy Act 2010.

[14] Zhou Guangquan, The Scope of Criminal Liability of Internet Servicers, 2 China Law Review (2015).

[15] Civil Judgment (2011) Z.L.M.Z.Z. No. 40 issued by Zhejiang Province Lishui City Intermediate People's Court.

[16] Civil Judgement (2006) Y.G.F.M.S.Z.Z. No. 355 issued by Guangdong Province Higher People's Court.

or regulation and infringing other's civil rights, that the ISP will bear too heavy legal burden, being difficult to advance. The unceasing change of legal obligation would make the ISP not know what course to take. Even more, the criminal punishment like the Sword of Damocles overhead makes the ISP be in a constant state of anxiety, thus definitely limiting the healthy development of internet technology and internet service industry tremendously. Therefore, it's not suitable for the ISP to assume the pre-review and concurrent monitoring obligation but only the ex post reporting and deleting obligation. Moreover, the ISP's reporting and deleting obligation is passive, which means that the ISP has no obligation to proactively review or monitor the internet content. Such obligation is just a general obligation imposed on the ISP, that is to say, in a field where there is no special legal provision, the ISP assumes no special management obligation.

To clarify the scope of the ISP's internet management obligation is a precondition of determining the ISP's criminal liability. For example, according to Amendment IX to Criminal Law, one of conditions for prosecuting the ISP is its failure to make correction after a supervisory authority orders it to take corrective measures. Then, does a supervisory authority has the power to give ISP an abstract order about corrective measure such as „illegal information is not allowed to appear next time", „please carry out real-time monitor over illegal internet information and delete it upon its emergence"? This paper gives a negative answer. The reason is that such abstract order about correct measure essentially requires the ISP to monitor the internet content at all times, thus practically transferring the review and monitoring obligation originally not assumed by the ISP to the ISP and increasing the ISP's legal obligation without legal foundation. A supervisory authority can only ask the ISP to delete illegal information such as violent or terrorist information or sexual photos which have appeared on its website. The scope of „correction requirement" shall be based on the following two points: the first one is that the corrective measure must be a specific and targeted requirement of deleting or preventing some type of illegal information. The second one is the corrective measure is targeted at practical and objectively existing illegal information rather than future and possibly emerging illegal information. The ISP will not take any criminal liability for failure to implement or complete such kind of correction required by a supervisory authority.

III. Foundation for Criminal Liability: Establishment of Online Content Management Obligation Based on Classification of Internet Services

The internet service, in broad sense, includes all types of service constituting and guaranteeing the normal operation of the internet, with extensive content and various types. The ISPs include those who utilize public tele-communication infrastructure to connect service node with internet backbone and then provide basic hardware service of internet access such as China Telecom and China Mobile, those who provide internet end-users with broadband installation, internet test and reparation and other services such as network technology companies in the market, and internet cache providers by means of WEB cache re-direction technology, as well as platform providers who are internet servicers creating internet space for content providers to publish information, for example the commonly-seen operators of BBS, microblog and other internet space. When a platform itself publishes information, it is also the content provider. In addition, the ISPs also include those who provide users with services such as online payment and

recharge, and providers of software engaging in one or more activities of transmission, receipt and representation.

In the internet information system, due to different service provided, each ISP enjoys different status in the internet system, ability of controlling information, likeliness of preventing illegal or criminal behaviors. Where the internet service content provided is different, the provider may face different legal obligation and punishment. For example, a pure internet content provider would not assume liability for the loss of data stored on the internet and an internet hardware access provider generally assumes no liability for illegal information emerging in the internet space. Therefore, it is a common practice all over the world to classify service providers according to their different service content provided and then set forth their respective criminal liability accordingly rather than impose a uniform criminal liability. For example, the Digital Millennium Copyright Act of USA[17] (hereinafter referred to as DMCA) classifies internet servicers into (1) those providing transitory digital network communications[18]; (2) those providing system caching service[19]; (3) those providing information residing on systems or networks at direction of users[20]; (4) those providing information location tools[21], and the Communications Decency Act defines the meaning of information content providers and accordingly sets forth their respective legal liabilities and constituents[22]. The Telecommunication and Media Act of Germany distinguishes service providers' functions and thus classifies internet servicers into content providers, access providers, caching providers and trusteeship providers[23], and establishes a liability system with different levels for different internet service providers. Where the internet service content provided is different, the provider's legal responsibility is different and the type of legal sanctions varies. In a situation where the law sets forth the criminal liability, the legal obligation of different service providers and the condition for constituting a crime due to failure to fulfil the aforesaid obligation are different.

From the criminal legislation practices in China, it is found that the legislator is not apt to adopt the mode of classifying the service content for distinguishing different ISPs' internet content management obligations and corresponding scopes of criminal liabilities and conditions for incrimination. Amendment IX to Criminal Law establishes a special rule of criminal punishment for the ISP's behaviour of failing to perform its legal obligation and creates a new mode of criminal lability of the ISP. The provision on the ISP's behaviour of failing to perform its safety management obligation sets forth three specific circumstances such as „resulting in wide spread of illegal information" besides the miscellaneous paragraph. In fact, in such three circumstances, not all legal obligations have the same source and different ISPs are involved. For example, „the wide spread of illegal information" is generally due to the platform provider' failure to perform its content management obligation of a website or information interactive communication platform, so the criminal liability shall not be imposed on operators providing internet hardware access service or caching service providers. As for „leakage of users' information resulting in serious consequences", the ISP providing information

[17] Digital Millennium Copyright Act.

[18] Above 20, 512(a).

[19] Above 20, 512(b).

[20] Above 20, 512(c).

[21] Above 20, 512(d).

[22] 47 U.S.C. §230(f).(3) (2006).

[23] Dieter Dörr, Steffen Janich（2011. *The Criminal Responsibility of Internet Service Providers in Germany*. *Mississippi Law Journal*, 80, 1247-1261.

storage generally assumes the criminal liability and other service providers have nothing to do with this. The responsible subject for „resulting in the loss of evidence of a criminal case and having serious circumstance" can only be the ISP providing data storage and having the obligation to store evidence. However, in practice, the smooth running of a network depends on normal operation of all components. Any behaviour of the ISP cannot be separated from other service providers' technological and equipment support. For example, in the circumstance of „resulting in the wide spread of illegal information", undoubtedly the first one who should assume the liability is the platform provider, but objectively the perpetrator cannot commit or complete its offence without the internet access service or access software service. The criminal liability cannot be extended without limitation to the ISPs in the interlocking internet service supply chain. At this point, there are some questions to answer: (1) Which type of ISPs is the competent subject of criminal liability? Where is the boundary of criminal liability? (2) Are legal obligations of and criminal constituents for different ISPs totally the same? At the level of criminal law, the legislation of China does not give clear clarification of ISPs nor define different ISPs' special legal obligations and corresponding criminal liabilities, so the consequence is that the scope of imposing criminal liability is not clear and the responsible subject is vague. The legislation may call all servicers providing various kinds of internet service as ISPs due to legislative technique, but during the application of judicial interpretation, it is unsuitable to vaguely and undistinguishably impose criminal liability on different ISPs, the criminal liability of which shall be judged on basis of the service content provided. The aim of classifying internet services is to define a certain ISP's role and status in the transmission, deletion or control of illegal information by specifying the difference among services provided by different ISPs, which is the precondition for judging whether the ISP has the internet content management obligation or assumes criminal liability or not.

IV. The Standard for Determining Criminal Liability: The Theory of Direct Control

The next question after solving the issue of classification of internet services is which approach and standard shall be adopted for determining different ISPs' content management obligations and subsequent criminal liabilities. For this, there are generally two directions in the academia. The first one is based on the traditional theory of joint offence and realizes the purpose of preventing the imposition of criminal liability on ISPs from expanding by limiting the radiative scope of the theory of joint offence. It's a common practice in both Civil Law and Case Law countries to hold the ISP criminally responsible as an accomplice. Till now, the USA also brings the ISP to criminal justice for imposing the accessorial liability according to the theory of joint offence. The famous case of BuffNET[24] opened a gate to prosecuting the ISP on the ground that the ISP provides electronic means or opportunity for the third party's criminal behaviour and thus „promote" or „assist or help" the illegal activity. The prosecutor may cite Title 18 of the U.S. Code to charge a website operator with criminal activities[25]. Prior to the adoption of Amendment IX to Criminal Law, the mode of the ISP's criminal liability in

[24] *Case People of the State of New York v. Buffnet*. 272 A.D.2d 982. 708 N.Y.S.2d 227, 2000 N.Y. Slip Op. 04475.

[25] Shahrzad T. Radbod, cited, p. 613.

China is similar to that in the U.S.A. In practice, it is the judicial interpretation states that the ISP assumes accessorial liability for its assistance in a cybercrime. For example, Article 7 of Interpretation of Several Issues concerning Legal Application in Criminal Cases of Making, Copying, Publishing, Selling or Transmitting Obscene Electronic Information by Use of Internet, Mobile Communication Terminal or information service center promulgated by the Supreme People's Court and the Supreme People's Prosecutor in 2004 and Article 6 of Interpretation (II) of Several Issues concerning Legal Application in Criminal Cases of Making, Copying, Publishing, Selling or Transmitting Obscene Electronic Information by Use of Internet, Mobile Communication Terminal or information service center promulgated by the Supreme People's Court and the Supreme People's Prosecutor in 2010impose criminal punish on ISPs for their crime-assisting behaviours such as internet access, server hosting, network storage space and communication transmitting channel. The Amendment IX to Criminal Law incorporates similar provisions scattered in many judicial interpretations and upgrades the level of such provisions through legislation. Meanwhile, it protects legal interests in advance and makes a crime-assisting behaviour become a principal offence. In essence, such legislation is not separated from the framework of existing criminal law theories or does not impose new legal obligation upon the ISP. However, in fact, the traditional theory of joint offence in China is insufficient to punish and govern ISPs because it cannot provide theoretical basis of justification in criminal regulation of ISPs' behaviours nor reasonably limit the combating scope. Therefore, the theories in China move towards different directions. Some scholars introduced the theory of neutral assisting-behaviour from Germany and Japan, trying to limit the scope of the ISP' criminal liability. Mr. Chen Hongbing introduced the analytic tool of the theory of neutral assisting-behaviour on basis of drawing on cases in Japan and Taiwan of China in the earlier time and holds that it's not suitable to punish the ISP as an accomplice if the assistance is neutral and does not create law-forbidding danger[26]. Around the adoption of Amendment IX to Criminal Law, Mr. Zhou Guangquan and Mr. Che Hao, according to such theory, reflected the reasonability of using criminal punishment as a means to punish and control behaviours providing IT support and hold that an apparently legal daily behaviours cannot be criminally punished just because the actor knows to some extent in individual situations that others may utilize those behaviours to commit a crime. The loss may outweigh the gain in terms of protecting legal stability and forming the legal order if the scope of an accomplice is excessively expanded[27]. On the whole, the theory of neutral assisting-behaviour derived from the framework of the traditional theory of joint offence holds the stance of restraining or limiting the participation and intervention of criminal law when judging ISPs.

In fact, the theory of neutral assisting-behaviour has obvious deficiencies in limiting or defining the ISP's criminal liability. Firstly, regarding the theory of neutral assisting-behaviour, there are many controversial opinions about the definition of a neutral behaviour and the standard of each opinion is very vague, thus receiving doubts about the operability. Secondly, in cyber space, it is impossible for the theory of neutral assisting-behaviour to distinguish different ISPs, hard to connect with the criminal liability system based on the classification of services, unable to realize the purpose of

[26] Chen Hongbing, *Research into the Punishability of Neutral Behaviors on the Internet: Centered on the Judgment of P2P Service Providers' Behaviors*, 3 Journal of Northeastern University: Social Sciences Edition (2009).

[27] Zhou Guangquan, *The Scope of Criminal Liability of Internet Servicers*, 2 China Law Review (2015).

limiting the scope of imposition of criminal liability. In a word, either the traditional theory of joint offence or the theory of neutral assisting-behaviour enjoys limited capability to explain the issue of ISP's criminal liability.

The second direction is to introduce other theories to explain and analyse the ISP's criminal liability. After the adoption of Amendment IX to Criminal Law, there emerged various views such as the Theory of Guarantor[28] and the Theory of Supervisory Negligence[29] when discussing the theoretic foundation for the ISP's criminal liability, and no agreement is reached. When the ISP refuses to perform its management obligation after being informed by a competent authority, the subjective state of mind is obviously not negligent, so the view of supervisory negligence is not accurate. Comparatively, „the Theory of Guarantor" could better solve issues of brining the ISP to criminal justice and limiting its criminal liability. Especially after the Amendment IX to Criminal Law imposes criminal liability on the ISP for its refusal to perform internet safety management obligation, it is particularly necessary to reasonably adopt the Theory of Guarantor to explain the ISP's criminal liability. According to the view of the Theory of Guarantor, whether the actor has the obligation to act depends on whether the actor enjoys the status of a guarantor. Only when the actor is the person enjoying the status of a guarantor and is able to perform the guaranty obligation, but fails to perform it resulting in hazardous consequence, is there omission equivalent to an act[30]. The huge advantage of the Theory of Guarantor is the matching and connectivity between the ISP's status of a guarantor, the ability to perform special guaranty obligation and the ISP's status and role in managing and controlling internet information, thus reasonably delimiting the scope of the ISP's criminal liability on basis of classification of internet services. That is to say, the ISP's objective capability to get access to and control information determines the existence and the size of the ISP's obligation to monitor or delete illegal information and whether an offence of omission is formed[31]. Therefore, this paper holds that the standard for determining the existence of the ISP's obligation of managing internet illegalities and crimes and the ISP's criminal liability is such service provider's direct control over illegal and criminal information. Such standard contains the following several meanings: Firstly, the ISP has control over illegal and criminal information and decides whether certain illegal or criminal information can be transmitted through certain channels and within certain scope. The service provider is not responsible for safety management regarding illegal and criminal information beyond its influence and control. Secondly, the ISP's control over illegal and criminal information is direct. The term of „direct" may be understood from two aspects: (1) If an ISP has the capability to control over illegal and criminal information and such control is not direct but needs help or intermediation of other ISPs, the former ISP's management obligation in terms of criminal law and criminal liability shall be denied. (2) In the chain of information transmission and dissemination, the ISP is only responsible for the illegal information of the first link and level under its direct control. The purpose of the standard of direct control is to limit the scope of imposition of criminal liability and

[28] According to the Theory on Guarantor, both the Crime of Assisting Implementation of Online Criminal Activities and the Crime of Refusing to Perform Internet Safety Management Obligation can be understood as offences of omission and accomplice.

[29] Lu Xu, *On the ISP's Criminal Liability and Related Issues*, 6 Research on Rule of Law (2015).

[30] Gong Houjun, *On the Evolution of the Theory on Guarantor and Its Enlightenment*, 4 Studies in Law and Business (2007).

[31] Yang Caixia, *New View on Omission Cybercrimes*, 2 Seeker (2007).

prevent the criminal liability from expanding even unlimited imposition along with the causal chain. Thirdly, the standard of direct control cannot be violated unless major social public interest is involved and such situations must be statutory and have clear basis in legislation.

V. Miscellaneous Issues Related to Determining the Criminal Liability

As for objectively hazardous consequence of the wide spread of illegal information, not all ISPs shall undertake the same criminal liability. The ISPs shall be distinguished according to different types of services they provided and their criminal liabilities shall be analysed specifically. The content generators are unexceptionally responsible for the content published in the cyber space whether it is on their own computers or on other severs. In addition, according to the general rule, the content providers assume the full responsibility regardless of the fact whether they have the right of copy or use[32]. The punishing rules all over the world are basically the same with differences that some countries punish the content provider by regarding it as one of ISPs, while some countries independently enact criminal rules other than those on the ISPs. Except for the content provider, other service providers assume different criminal liabilities on basis of different content management obligations. The specific analysis is as follows:

(I) Criminal Liability of the Internet Platform Provider

The criminal liability of the internet platform provider, different from that complete and unexceptional criminal liability of the content provider, is limited and conditional. The platform service provider assumes no criminal liability for the content generated by others, but shall be criminally responsible for failure to perform subsequent obligations after being given effective notice. However, under certain circumstances, the platform provider may have its identity changed due to participation in generating the internet content and thus assume the criminal liability of the content provider.

The precondition for the ISP being immune from civil and criminal liabilities is that the illegal internet information is uploaded by a third party but generated by the platform provider itself. Then, does the fact that the content is uploaded by a third party ensure the internet platform provider's immunity? The judicial practice has the tendency to hold the stance of strict interpretation and limited scope. It is generally believed in the judicial practice of China that the ISP shall be regarded as a content provider and assume corresponding legal liabilities if it edits or amend information uploaded by others or change the receivers[33]. Other countries such as Germany adopt the similarly same stance. The U.S.A. adopts a stricter mode for limiting the application of the ISP's immunity when the ISP participates in generating the internet content. In the famous case of Roommates.com[34], the court excluded the application of Section 230 on the ground that users are required to complete a questionnaire including users' gender, sexual orientation and other personal information. The court held in this case that the website actually served as an information and content provider[35]. Therefore, the ISP's

[32] Koch, CR 1997, 193 (197); Spindler, NJW 1997, 3193 (3196); Pelz, ZUM 98, 530(532).

[33] Judgment (2011) Z.L.M.Z.Z. No. 40 issued by Zhejiang Province Lishui City Intermediate People's Court.

[34] Roommates.com, LLC, 521 F.3d 1157, 1161 (9th Cir. 2008) (en banc).

[35] Roommates.com, LLC, 521 F.3d 1164 (9th Cir. 2008) (en banc).

participation in generating the content may result in its identity shift towards a provider and the content management obligation. Under such type of situations, the internet platform provider shall assume corresponding criminal liability as an internet content publisher or provider.

Shall an internet platform assume the criminal liability of the content provider if the platform does not directly provide information but presents links to illegal information? In Germany, there are a lot of controversies over this issue. Generally, the link is only regarded as an intermediary for getting access to external content. However, case differences shall be considered. If a platform explicitly expresses its approval of the linked content, such external content provided by others may be regarded as provided by the platform itself. Meanwhile, when making such decision, the quantity of the linked content and data shall be taken into account. If a platform generally and massively cites others' data or documents, the content provided by others cannot be regarded as provided by the platformed. If those who setting the link accept (external) content as their own content, they will be punished for an assisting behaviour. However, if there is a further link in the cited website, the criminal liability shall not be extended to the link of the second tier[36]. It is obvious that Germany holds a relatively looser stance in the platform service provider's identity shift. This paper agrees on that the platform provider shall not assume responsibility for the content generated in the link of the second tier or above because the service provider has no direct control any more. However, the platform provider participation in generating the content is not a behaviour simply guiding user's access but a real transmission[37], so excessively loose standard of legal application isn't beneficial to the effective control of illegal information. More importantly, when a platform provider participates in generating the content, it has complete autonomy and control in choosing to provide or not to provide relevant links without restriction. In addition, such choice may not increase any extra business cost of a platform provider. From the perspective of balance of interest, it is not unsuitable to hold the platform provider responsible for this. Therefore, the platform provider shall undertake the duty of care for its behaviour of providing the first-tier link, know the linked content and assume corresponding criminal liability because the intermediary for assess is provided by the platform.

(II) The Software Assess Provider's Criminal Liability

A software assess provider refers to a software provider engaging in one or more activities such as transmission, receipt, exhibition, forwarding, search[38]. The attention-focused QvodPlayer case is a suitable example for discussing this issue. The prosecutor argued that the QvodPlayer provides internet videos publishing, searching, downloading and playing services on basis of streaming media technology and by means of publishing free installation program of QVOD media server and QvodPlayer player software in international internet. The prosecutor considered that the QvodPlayer company and persons in direct charge, knowing that users use installation program of QVOD media server and QvodPlayer player software for obscene videos, let them alone and result in

[36] Flechsig & Gabel, CR 1998, 351 (356); Lhnig, JR 1997, 496 (498); Park, GA 2001, 23 (32); Gehrke, ZUM 2001, 34 (39); Spindler, MMR 2002, 495 (503); SIEBER, supra note 14, at pt. 308. Contra Lackner& Kahl, pt. 7b.

[37] Yu, Zhigang, *The Criminal Law Theory in Virtual Space*, China Fangzheng Press (2003), 185.

[38] 47 U.S.C. §230(f). (4) (2006).

wide spread of mass obscene videos on the internet[39]. In this case, the prosecutor's train of thought is that the QvodPlayer company and the persons in direct charge are accomplices of the crime of the dissemination of obscene materials for a profit[40]. Some scholars question the necessity and reasonableness of criminally punishing such type of behaviours of QvodPlayerwhich apparently seems neutral and harmless but objectively helpful to the criminal, and hold that it should be prudent to punish neutral assisting-behaviours, the scope of which criminally punished shall be limited as far as possible[41].

The issue discussed herein is whether a provider of assess software such as QvodPlayer shall assume criminal liability of an ISP for the wide spread of illegal information under the framework of Amendment IX to Criminal Law. This paper holds the negative view on the ground that roles and statuses of assess software in internet service system are not the same. After an access software is published, the provider loses control over users' using behaviours and modes of use. The use of the software by users is independently from the software provider, so the software provider shall not assume criminal liability for users' behaviours. However, it's a different case for the internet platform. Because the internet platform is always under the control and dominance of the platform provider and the platform provider has special obligation to manage the content in the platform, the platform provider shall assume corresponding criminal liability when requirements are satisfied. In fact, an access software provider and an internet hardware access provider enjoy the similar roles and statuses, both objectively acting as one of conditions for disseminating illegal information. Not all ISPs providing information dissemination conditions but those directly controlling illegal and criminal information shall be included in the scope of criminal liability, otherwise all parties related to internet service even computer producers and sellers are possibly punished criminally. This is obviously ridiculous.

(III) Criminal Liabilities of Other ISPs such as Internet Hardware Assess and Cache Providers

Generally, the internet hardware access and cache provider will not be held criminally responsible for the use of its access and cache service by uses. However, the hardware and cache service provider's immunity from criminal liability is not absolute. For example, Item 2 of Paragraph 1 of Section 8 of Telecommunication and Media Act of Germany states that the privilege (immunity from criminal liability) is not applicable if the service provider intentionally collaborates with served users to commit illegal activities. Such collaboration is not necessarily between a provider and an user, but it can be between providers who act as joint offenders[42]. There is a similar provision in China. Article 7 of Interpretation of Several Issues concerning Legal Application in Criminal Cases of Making, Copying, Publishing, Selling or Transmitting Obscene Electronic Information by Use of Internet, Mobile Communication Terminal or

---

[39] Gao Jian, *Haiding District Court Accepting the QvodPlayer Case Involving Pornographic Materials*, Beijing Daily, Feb. 11, 2015.

[40] There are also some scholars considering that in such circumstance, the actor shall be regarded as the principal offender of the crime of dissemination of obscene materials for a profit, i.e. an accomplice becoming a principal.

[41] Che Hao, *Who Shall Be Responsible for the Consequence of Neutral Behaviors in the Internet Age*, 1 China Law Review (2015).

[42] Theodor Leckner et. al. § 184 pt. 58, in Adolph Schonke, Horst Schroder, *Kommentar zum Strafghesetzbuch* (2006).

information service center promulgated by the Supreme People's Court and the Supreme People's Prosecutor in 2004 sets forth that the actor, knowing that another person commits an offence of manufacturing, coping, publishing, selling or disseminating obscene electronic information, provide assistance such as internet access, server hosting, network storage space and communication transmitting channel and expense settlement, is regarded as a joint offender. It should be noted that the aforesaid „knowing" is specific and targeted and shall not be abstract, that is to say, the access service provider has the intention to commit a crime jointly with another person (collaboration). As everyone knows that the existence of illegal information in cyber space, the access and cache service provider could not have been unaware of such internet access service will objectively result in the dissemination of illegal information. If the „knowing" is required to be abstract rather than specific, any internet access and cache service will definitely constitute a crime. This is obviously not what we hope.

In the context of Amendment IX to Criminal Law, the internet hardware access and cache service provider shall be criminally responsible for the wide spread of illegal information arising from its failure to implement an internet supervisory authority's order and refusal to make correction. However, it should be noted that due to the specialness of internet access service, the scope of access service is more extensive than the platform service and the social influence is huger, involving many interested parties, an order issued by a supervisory authority shall be strictly limited. This paper holds that only there is a risk of spreading information constituting serious crimes such as endangering national safety or public safety, can a supervisory authority issue an order to ask the hardware access service provider take measures. In addition, it is formally limited to the clear expression in a law.

References

1. Caixia, Yang, *New View on Omission Cybercrimes*, 2 Seeker (2007).

2. *Case Doe v. MySpace*, Inc., 528 F.3d 413 (5th Cir. 2008).

3. *Case of Scarlet v. SABAM,* Court of Justice of the European Union, Judgment of the Court (Third Chamber), 24 November 2011, In Case C□70/10.

4. *Case People of the State of New York v. Buffnet*. 272 A.D.2d 982. 708 N.Y.S.2d 227, 2000 N.Y. Slip Op. 04475.

5. *Case Stoner v. eBay*, Inc., No. 30566, 2000 WL 1705637, at *3 (Cal. Sup. Ct., Nov. 1, 2000). 141 Cong. Rec. H8468-69 (daily ed. Aug. 4, 1995) (statement of Rep. Cox).

6. Case *Zeran v. America Online*, Inc., 129 F.3d 327 (4th Cir. 1997).

7. Civil Judgement (2006) Y.G.F.M.S.Z.Z. No. 355 issued by Guangdong Province Higher People's Court.

8. Civil Judgment (2011) Z.L.M.Z.Z. No. 40 issued by Zhejiang Province Lishui City Intermediate People's Court.

9. Dörr, Dieter, Janich, Steffen, 2011. *The Criminal Responsibility of Internet Service Providers in Germany*. *Mississippi Law Journal*, 80, 1247-1261.

10. Gorman, Robert A., Ginsburg, Jane C., 2006. *Copyright: Cases and Materials (*7th ed.*)*, Foundation Press.

11. Guangquan, Zhou, *The Scope of Criminal Liability of Internet Servicers*, 2 China Law Review (2015).

12. Hao, Che, *Who Shall Be Responsible for the Consequence of Neutral Behaviors in the Internet Age*, 1 China Law Review (2015).

13. Hongbing, Chen, *Research into the Punishability of Neutral Behaviors on the Internet: Centered on the Judgment of P2P Service Providers' Behaviors*, 3 Journal of Northeastern University: Social Sciences Edition (2009).

14. Houjun, Gong, *On the Evolution of the Theory on Guarantor and Its Enlightenment*, 4 Studies in Law and Business (2007).

15. Jian, Gao, *Haiding District Court Accepting the QvodPlayer Case Involving Pornographic Materials*, Beijing Daily, Feb. 11, 2015.

16. Judgment (2011) Z.L.M.Z.Z. No. 40 issued by Zhejiang Province Lishui City Intermediate People's Court.

17. Lawrence G. Walters (2012), *Shooting the Messenger: An Analysis of Theories of Criminal Liability Used Against Adult- Themed Online Service Providers*, in Stanford Law and Policy Review, 171, 10.

18. Leckner, Theodor et. al. § 184 pt. 58, in Adolph Schonke, Horst Schroder, *Kommentar zum Strafghesetzbuch* (2006).

19. Roommates.com, LLC, 521 F.3d 1157, 1161 (9th Cir. 2008) (en banc).

20. Roommates.com, LLC, 521 F.3d 1164 (9th Cir. 2008) (en banc).

21. Xu, Lu, *On the ISP's Criminal Liability and Related Issues*, 6 Research on Rule of Law (2015).

22. Yen, Alfred C. (2000). *Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise Liability, and the First Amendment*, The Georgetown Law Journal, 88, 4.

23. Yu, Zhigang, *The Criminal Law Theory in Virtual Space*, China Fangzheng Press (2003), 185.

24. Zhou Guangquan, *The Scope of Criminal Liability of Internet Servicers*, 2 China Law Review (2015).