Advances in Social Science, Education and Humanities Research, volume 615
Proceedings of the 2021 4th International Conference on Humanities Education and Social Sciences (ICHESS 2021)

Analyse the Penalty Limits of the Provider of P2P Sharing Technology
In the Case of Qvod

Chengcheng Guo*

[1] *College of Art & Social Science, Australian National University, ACT, Australia, 2601.*
[*] *Corresponding author. Email: u6398337@anu.edu.au*

ABSTRACT
The punishable boundary of P2P network sharing technology provider in the Qvod case is analyzed in this article under the administration of justice in China. The singular P2P technical pattern and a mixing P2P+CDN technical pattern are applied in Qvodplayer. The operation mechanism of Qvodplayer software is following: users share and spread video resources through P2P sharing, under the condition in which the network bandwidth is limited, or the transmission rate of video resources is slowed down, through P2P caching, hotspot videos are grabbed and cached by Qvodplayer through its dispatch server and caching server. Based on the running mode of Qvodplayer, as the technology provider, the server (Qvod Company) has become the secondary source of video resources that have already been uploaded. Thus, Qvod Company not only plays the role of technology provider, but it is also the provider and administrator of information service related to network videos. From the aspect of management, knowing that there are obscene videos in the software, Qvod Company still indulges their spread and benefits from them under the premise that it can perform the duty of supervision. Thus, Qvod Company fails to perform its duty of supervision and directly participates in the spread of obscene videos, which should undertake criminal liability in this case.

Keywords: *P2P, Qvod Case, Winny Case, Technical Neutrality, Helping Behaviour, Penalty Limitation.*

1. INTRODUCTION

The Peer-to-Peer (P2P) Internet communication technology has been progressively exploited to cybercrimes. For the efficiency, anonymity, ease of use, and negligible costs of the P2P, suitable digital platforms are created for cybercrimes (e.g., copyright infringement and dissemination of virus) to establish botnet and darknet. P2P networks can be applied in several manners (e.g., distribution computing, collaboration, and communication), while file-sharing is the most famous function is supported by the P2P technology. Since the P2P network can conveniently share files, it has been popularized as impacted by the unauthorized distribution of copyright documents. The design and implementation of the P2P file-sharing system stress three identities, i.e., centralized/decentralized/hybrid, open-source/proprietary, and encrypted/unencrypted. The P2P network has undergone development with three generations emerged. The mechanism of the first-generation P2P network requires the central server to present the catalog of resources and IP addresses of peer computers. For the second generation, the decentralization and fragmented caching system act as the essential characteristics. The third-generation P2P network has developed a mature and flexible digital sharing system. The high-speed and stable dissemination, anonymity, the low-cost setting system, and the fragmented mode of transmission create a convenient and safe digital environment to achieve network resource sharing.

In Western World, three influential P2P systems had been launched in the late 1990s (i.e., Napster music sharing system, Freenet anonymous data store, and SETI@home distributed volunteer-based scientific program). In Eastern nations, the typical cybercrimes associated with P2P networks include the Qvod case, the Winny case, and the Kuro case. Compared with the Winny case and the Kuro case, the Qvod case highlights the disseminating obscene articles for profits. Both the Winny case and the Kuro case are exploited to the copyright infringement. Furthermore, in most cases, the P2P network provider acts as the pure technology supporter without any subjective intention for crimes,

which can be applied in technical neutrality. In the Qvod case, the Qvod Company has acted more than a technology provider. It also serves as the manager to monitor the dissemination of obscene materials using Qvodplayer software.

2. BACKGROUND

Heated discussions and concerns on the criminal liabilities of the technology neutrality principle and the neutral cyber help had been caused after the first instance of the Qvod case. Cybercrime in the context of P2P shared network technology was tried. During the trial, the defendants defended themselves by bringing out the idea of "technology is innocent" [1]. Besides, they considered Qvod as the video player, simply providing the P2P video support and caching service to improve network transmission efficiency to users instead of acting as the party publishing obscene videos [1]. By complying with the technology neutrality principle, the acts of Qvod Company should be applied to the International Safe Harbor Principles, and only the obscene videos in caching dispatcher should be deleted. However, in this case, the defendants were sentenced based on illegally making profits from disseminating obscene articles acquired from caching-only name servers and the P2P shared network and cache scheduling of hot videos used by Qvodplayer technologically assisted the dissemination of obscene articles. As supported by P2P, Qvod Company, the service provider, blurred the relationship between resource provider and user. It served as the secondary source of uploaded resources for its distinctive caching technology [2]. Qvod Company, a service provider in its P2P shared network, could control the caching, searching and recommendation of resources compared with conventional network video players.

In another similar case, i.e., the Winny case in Japan, P2P was involved as well. These two cases, however, remain fundamentally different. Winny refers to resource-sharing software. It exploits P2P without the intervention of any central server, which creates a network with computers of equal status [3]. As opposed to Qvodplayer, Winny simply uses P2P sharing, while it does not have any caching scheduling server. In this case, defendant Isamu Kaneko was only the P2P service provider, while Qvod Company was the technology provider and the provider and manager of network video information service [3]. For the mentioned reason, from the technological perspective, two network service structures were adopted by using Qvodplayer, i.e., P2P sharing and P2P caching, while only P2P sharing was employed by Winny [4]. Even though both cases involved the support of a P2P shared network, Qvod Company and its defendants were found guilty of disseminating obscene articles for profits. Nevertheless, the defendant in Winny's case was acquitted of a charge since the trial acknowledged the value-neutrality and the helping nature of Winny. There was a lack of subjective motive [3].

The resource scheduling and caching scheduling of hot videos of Qvodplayer as a typical symbol of P2P shared network technology had gone beyond the third-generation conventional P2P network. Thus, this study starts from the Qvod case to investigate the role of P2P shared network users in his helping acts and discuss the boundaries of the criminal liabilities a provider of P2P shared network shall undertake.

3. LITERATURE REVIEW

3.1. Comparison and Analysis of Qvodplayer and Winny Software e

Qvodplayer software exhibits two network technical characteristics, i.e., pure P2P mode and P2P+CDN (Content Delivery Network) mode [5]. The pure P2P mode refers to a P2P network shared transmission mode with a central dispatch server as the core. The pure P2P mode only develops a file transfer link between users via a centralized dispatcher. Thus, the transmission speed will slow down if the network bandwidth limit is received, and this circumstance makes it difficult to meet the user's viewing needs. Accordingly, Qvodplayer adopts the second P2P+CDN model to directly participate in the file transfer. CDN network technology is capable of integrating user-oriented information and connecting users to the nearest node by complying with the network traffic and the link load of each node and the distance and response time of the user [5]. The aim is to allow users to acquire the required content nearby, improve users' response speed, and solve a series of effects exerted by network congestion [5]. In other words, the cache server will not intervene in the transmission under the sufficient transmission bandwidth between users. For a central scheduler and a cache scheduler, Qvodplayer has lost the decentralized characteristics of the conventional third-generation P2P technology.

Qvodplayer's network system operation mode exhibits two characteristics. One is a centralized P2P network information sharing system. The other is that Qvodplayer can control the video storage of the cache server and the behaviour of providing videos to users via the scheduler. Thus, the dispatch server and cache server of Qvodplayer is of higher significance for disseminating obscene materials than its P2P network sharing technology. Under the P2P+CDN technology model, Qvodplayer adopts the dispatch server and cache server to grab and cache hot videos and provide them to on-demand users for viewing. Such a series of actions endow Qvodplayer with a novel identity other than the network technology provider, which is the manager of video resources. Hence, Qvod Company is obliged to review and screen the content of cached videos and prevent the

spread of obscene videos. However, Qvod Company had been informed that it was involved in the spread of obscene videos before the incident. Since users use the software to spread obscene videos, Qvod Company fails to fulfill the administrator's obligations and still provides users with obscene videos via the cache server. Meantime, though the Qvodplayer itself is free, the software comes with some paid items. It is profitable.

Inconsistent with Qvodplayer software, Winny software is file-sharing software that exploits P2P network technology to exchange information resources without any charge items. It is completely free and requires not any intervention of a central server. The developer of Winny software, Kaneko Isamu, was indicted by the Kyoto District Court of Japan by the Public Prosecutor's Office for helping to infringe copyright [6]. Given the technological innovation and social impact of the novel generation of the P2P technology, the court of the first instance took two and a half years to make a judgment in December 2005, imposing a fine of 1.5 million Japanese yen [6]. Afterward, both the second and third trials recognized the value-neutral nature of Winny software and claimed that the defendant Kaneko Isamu was acquitted.

Winny software refers to P2P download software by complying with the third-generation P2P technology for secondary development. Compared with the existing generation of the P2P software, the resource sharing of Winny software is not limited to audio and video but includes most types of data files (e.g., documents, compressed packages, pictures, and executable files) [3]. Winny software exhibits extremely high confidentiality; it can encrypt the IP address of each user to ensure the anonymity of users when exchanging files [3]. Moreover, it exhibits the characteristics (e.g., decentralization, multiple downloads, and automatic downloads), thereby enabling efficient and secret transmission of data information. The mentioned characteristics cause Winny software to be subject to a high risk of infringing on authors' rights. As the software developer, Kaneko Isamu is the provider of the network technology and has the responsibility to supervise the illegal use of the software. Accordingly, when Kaneko Isamu disclosed the Winny software, it posted a warning on its website that "do not use this software for the exchange of illegal files" [3]. Compared with the Qvod case, the Winny case applies to the principle of technology neutrality for the following reasons. 1) Kaneko Isamu did not offer any server but P2P software only. 2) Kaneko Isamu had not been informed by others that the software he had developed was adopted to infringe the copyright of others; he had not recognized that the software was illegally used to infringe copyright. Thus, there is no subjective intention. 3) The free resource sharing platform of Winny software neither publishes advertisements nor pays to download, with no profit-making purpose.

3.2. P2P Sharing and P2P Caching in the Qvod Case

As supported by pure P2P mode and P2P+CDN technology mode, Qvodplayer forms two network architectures, i.e., P2P sharing and P2P caching. First, P2P sharing takes the central dispatch server as the core. The user (webmaster) selects the release file to be released, generates the feature code of the video via the Qvodplayer resource server program, and exports the link to the Internet. When the user clicks the link to play the video, the link will be passed to the P2P component of the player via the Qvodplayer plug-in on the browser. The P2P component obtains the online users with the feature code from the central dispatch server by complying with the feature code in the link and then connects with these users to be watched. P2P sharing merely conducts the data sharing and the mutual transmission between users. The central dispatch server is capable of dispatching all clients and cache servers [1].

Second, P2P caching is based on the cache scheduling server. Qvod Company has set up over 1,000 cache servers in different operators nationwide. The cache scheduling server will instruct the server in the appropriate position to grab and store the video file when the number of on-demand video files satisfies a certain numerical standard. The essence of the cache server is a central server as well. The cache server can be automatically deleted in accordance with the pre-selected settings, or the video files in it can be deleted manually [4]. Besides, a certain connection is developed between P2P sharing and P2P caching. When the user exploits the Qvodplayer to search for a video, the cache scheduling server will query the cache server to check whether the video is stored. When both the network user's shared resource and the cache server own the video resource, the download path under P2P sharing will be limited by bandwidth, and the download speed will be low. Then, the cache scheduling server will provide the optimal download path, allowing the user to retrieve and download the video from the cache server. The cache scheduling server is capable of downloading, storing, and providing videos. Qvod company decides whether to cache or not according to the number of times the video is on-demand. This number of times may be adjusted continuously owing to the number of users of the network access service provider and the available storage space of the server providing the cache service.

As supported by the pure P2P technology mode, Qvodplayer only offers P2P sharing network services. The Qvod Company is merely a provider of P2P network sharing technology. In this context, Qvodplayer only offers users a video resource-sharing platform. There is no subjective intention for disseminating obscene videos, and Qvod Company does not have conscious and active behaviors [5]. Thus, the software can apply to the principle of technological neutrality. However, the main

operating mode of Qvodplayer is P2P caching network service supported by P2P+CDN technology. P2P caching is a key network service framework operated by Qvodplayer. Moreover, the judgment on the Qvod case focused on active P2P caching services instead of P2P distributed sharing services [4].

Under the network service framework of P2P caching, Qvodplayer 's scheduling server and cache server are involved in the process conducted by users to publish or order online videos and accelerate the on-demand download of the video. Accordingly, Qvod Company was given the identity of the video resource provider and manager. In other words, the pure P2P mode is only an explicit behavior, which is developed to help users watch videos. The P2P+CDN model implies Qvodplayer's 'storage-distribution' operation model for popular videos [5]. To be specific, the central scheduler serves as the connection point between the storage and distribution modes. The cache server can store and provide video only in the role of the central scheduler [5]. Since the operation of the cache scheduling server should rely on the data and instruction mechanism of the central scheduler, Qvod Company, a manager, is capable of reviewing and screening the video content in the cache server via the central dispatch server and fulfilling its regulatory obligations. Besides, administrative agencies had punished Qvod Company for allegedly spreading obscene materials many times before the incident. However, Qvod Company still allowed obscene videos to spread by using the Qvodplayer subjectively and knowingly, with an indirect intention. Moreover, based on their supervision obligations, users can upload obscene videos, and servers are allowed to crawl and cache obscene videos for profit-making purposes, resulting in the act of practice. Given the above two points, the behavior of Qvod Company is separated from the basic attributes of the principle of technology neutrality. It cannot fit the principle of technology neutrality.

3.3. Case Brief and Conviction of Qvod Case

In September 2016, Haidian District Court implemented a trial on the Qvod case and determined in the first instance decision: "Shenzhen Kuaibo (Qvod) Technology Co., Ltd., Wang Xin, and other defendants gained an insight that Qvod internet service system was adopted to spread pornographic videos but refused to fulfil their obligations of supervision and intervention to expand businesses and make illicit profits, the Qvod Company indulged their established network service system in being tapped for spreading pornographic videos, which harmed society and broke the criminal law, the prosecuted Qvod Company and the defendants shall be investigated for criminal responsibility abiding by the law" [7]. The main operations mode of Qvod Company was to provide users with free video player software (Qvodplayer) and resource server software (QSI, Qvod Server Install) to watch various videos.

From the technical perspective, Qvodplayer adopts P2P streaming media technology characterized by distributed network resource sharing. It enables any user (head of the station) to generate hash values via the resource server and export the link containing hash values to their own or others' websites. Then it shares videos with other users via the P2P Tracker; meantime, they can download video resources uploaded by other users [1]. Moreover, Qvodplayer created a Cache Tracker to capture and cache those popular videos with high clicks to accelerate the download of users and facilitate them to watch videos. Qvodplayer adopted a self-running or cooperative operation pattern and established 1000 Cache Servers by employing various operators in multiple locations nationwide [1]. When the click rate of some videos reaches a certain figure, the Cache Tracker will order a Cache Server in a suitable location to store this video resource. When the user clicks the link of these videos with a high click rate, the Cache Tracker will generate the optimal route for the user to access the videos from Cache Server under the low download speed. Since the obscene videos were among the most-viewed ones, the Cache Server would automatically store them. Though Qvod Company offered the software without charge of fees, the services (e.g., Qvod News, client, third-party software bundling, and VIP recharging) were non-complimentary projects. To be specific, Qvod News and third-party software bundling were the main projects for profits.

In August 2012, the Public Information Internet Security Supervision and Regulation Branch of Shenzhen Public Security Bureau (Shenzhen Internet Supervision Authority) warned Qvod Company as administrative penalty. They ordered immediate rectification since the company failed to establish Internet security, protection, and management systems and take security measures [1]. In response, Qvod Company established a "110" platform to filter and block illegal keywords and illegal videos. In contrast, this platform was shelved just after Shenzhen Internet Supervision Authority examined and accepted the platform. In August 2013, law enforcement officers from the Radio and Television Bureau in Nanshan District of Shenzhen investigated the company again and identified playable pornography in the software. The company submitted a rectification report and accepted the administrative penalty, whereas it still did not restart the blocking function at the "110" platform [1]. In the same year, as inspired by Wang Xin, Qvodplayer changed the storage mode of video resources in Cache Server by storing the original video document fragmentally. Therefore, it is suggested that multiple servers download one video, and each of them only stores it partially.

The sentence of the Qvod case can be analysed from the objective and subjective aspects of the act. First, the objective act of the crime of disseminating pornographic materials for profit is to broadcast and display porn videos or create websites on the Internet, so people can review and further spread them [8]. However, with the difference in ways to disseminate, the act by nature is to make non-specific people watch and feel pornography. Since Qvod Company captured and stored porn videos via its P2P Tracker and Cache Tracker and directly provided users with porn video stored in the Cache Servers, the company's act is considered to disseminate porn videos by displaying them. As ruled by the first sentence, Qvod Company, the internet video service provider, should assume the duty of Internet security regulation but failed to fulfil its obligation even it could. Qvod Company has to regulate users' review of porn videos after capturing those videos from the perspective of acts and omissions. In contrast, it still provided them for users via the Cache Server. If a doer directly and substantially dominates the criminal process and result, they shall be considered to play a vital role in the crime with act dominance [9]. Qvod Company, after capturing and storing porn videos by servers, provided them for users to review, rather than fulfilling its duty to supervise and regulate users or even take actions to prevent porn videos from further spreading. Based on the mentioned series of the act, Qvod Company, the main doer, held certain dominance in spreading obscene materials. The analysis from the perspective of dominance demonstrated the acts and omissions when Qvod Company disseminated obscene materials.

Second, from the subjective perspective, Qvod Company, before the first sentence, had clearly known porn videos existing in its Cache Tracker for profits. The subjective awareness of Qvod Company can be referred to as the investigation conducted by law enforcement officers from the Radio and Television Bureau in Nanshan District of Shenzhen in August 2013. As indicated from the investigation result, Qvod software existed the tracing of obscene videos, and the company was given an administrative penalty. Wang Xin knew the existence of pornography in Cache Servers, whereas he was still inspired to change the video storage mode in the servers. Though Qvod did not gain profits from users who provided porn videos or those downloading them, the popularity of those videos has brought advertisement gain to the company. As a result, Qvod Company is intended to make profits subjectively. In brief, according to the case brief of the Qvod case, Qvod Company was the provider of Internet video and information service, as well as the supervisor and regulator of videos, so it could undertake the duty of reviewing, blocking illegal content, and preventing the spread of obscene videos.

4. THE PENALTY LIMITS OF P2P TECHNOLOGY PROVIDER IN NETWORK HELPING BEHAVIOR

4.1. Technological Level

Technology is innocent in its nature, regardless of P2P sharing technology or P2P network cache service. For example, in the Qvod case, P2P network cache service, as the network cache technology, is disseminated from a technical perspective and the route automatically generated based on certain network technology principles. In other words, the dispatch server is limited to capturing certain videos and assigning them into cache in line with the predefined technological mechanisms, rather than judging the legitimacy of those videos [10]. Therefore, P2P network cache is classed as passive action rather than the behavior of dissemination from a legal point of view [10]. Without the intent of dissemination, conviction can't be made. Under the pure P2P model, Qvod Company assists the practice of dissemination by providing users with a player that can be used to watch videos. With the support of P2P+CDN, Qvod Company gets involved in the practice of dissemination. The caching server directs popular videos into the cache according to the orders issued by the central dispatch server and makes them available to view for users. In the course of dissemination, Qvodplayer has consciously contributed to the efficient dissemination of pornographic videos. Thus, Qvod Company permits and gets involved in the dissemination of pornographic videos [5]. It is the provider of this technology and the provider and administrator of those video resources. From a technical perspective, the behavior carried out by Qvod Company represents its actions.

In essence, Qvodplayer can block the dissemination of pornographic videos through technical means. There are two features manifested because the CDN module adopted by the Qvodplayer is updated based on BT software developed by Zhang Kedong, who is the technically responsible person for Qvodplayer [5]. Firstly, Qvodplayer is a P2P network service system equipped with a central server. Secondly, caching service operates under the dispatch by Qvodplayer. P2P document sharing can be categorized into centralized indexing, decentralized indexing, and the super node model in between according to the degree of concentration and decentralization shown by indexing. Due to the heavy reliance of Qvodplayer on the central dispatch server, Qvodplayer adopts the centralized indexing model. Thus, it is believed by the author of this paper that Qvodplayer could apply index technologies in the dispatch server and caching server to set keywords for filtering out certain illegal videos. Then it makes use of the automatic-deleting and auto-blocking technologies in P2P sharing network to monitor the illegal videos automatically and continuously. Besides, Qvodplayer

can monitor and prevent users from uploading illegal videos by putting in place the real-name network mechanism and imposing restrictions on the anonymous visit made by users. These technological measures require those network platforms to keep updating how censorship is practiced as technology develops, with a shift from manual censorship to technology-driven censorship. However, the upgrading in this form does not mean that the providers of network technologies will cease to be responsible for censorship. On the contrary, there is a change to how their responsibilities are performed, that is, to maximize the combination of technology and law with data.

4.2. Management Level

From the perspective of management, Qvod Company fails to carry out technical censorship properly to the extent that its obligation of network security management is fulfilled. In the Qvod case, the company does not fulfil its obligation of carrying out supervision, which is the core of its illegal acts [7]. Besides, from the technical perspective, the company has the duty of taking advanced action against disseminating pornographic videos, which makes it obligatory to block the dissemination of pornographic videos and remove illegal videos from its servers. Qvod Company, as the provider and administrator of its P2P sharing technology, can fulfil its obligation of censoring various illegal contents after its servers capture the popular videos and then present them to its users. This company is supposed to have taken effective measures to censor and remove those pornographic contents, which is the obligation placed on the provider and administrator of network service and online videos to ensure the orderly operation of the entire online space. However, Qvod Company fails to fulfill its obligations. On the contrary, while knowing that those popular videos captured and stored by its caching servers are pornographic, this company still allows its users to share and watch pornographic videos and even present its users with pornographic videos through its caching servers for profits. These behaviors performed by Qvodplayer constitute inaction. Thus, this company is guilty of intentional misuse and improper censorship of P2P network technologies. It is not justifiable either to use 'technology is innocent' for self-defense or incite the principle of technological neutrality. In combination with the technical characteristics of the case involving Qvod Company, the conditions of applying the 'technology neutrality principle in the P2P network technology can be classified into subjective conditions and objective conditions.

Based on the principle of technical neutrality, if a product carries technological innovation and its application is for legitimate purposes without constituting substantial infringement, the offering of this product is deemed legal. In this case, and the company should not take legal responsibility for the infringement [11]. Therefore, the preconditions for Qvod Company to apply the "technology neutrality" principle as the objective condition for self-defense include substantial non-infringement purpose, the low dependence on the central dispatcher, and the capability of censoring and preventing users' illegal acts. Meanwhile, the subjective behaviors of the defendant should also meet the following conditions: the non-dominance over infringement by users, no profits made out of the infringement, and other illegal acts except for the infringement of copyright. For the providers of network service, the statutory responsibilities of censorship and investigation are passive. According to Article 286 of the Criminal Law of China, one of the explanations for the crime of refusing to fulfill the obligations of network security management of network service providers mentions that "refusal to correct although the supervision department has ordered it to take corrective measures," [12]. The explanation of this criminal law implies that the obligation of the network service provider in the level of legal liability is a passive form, which the obligation is generated after the cognition of the existence of illegal content [13]. Thus, the active obligation of security management and censorship is a form of social responsibility for network service providers. In the constant process of technological innovation, the provider of network service ought to evaluate how this technology will put society at risk to ensure that it can fulfill its social responsibility as a service provider. Particularly, the constant upgrading of Internet technologies may cause the means of censorship to lag behind. In other words, the development of Internet technologies has far outpaced the upgrading of censorship. Thus, network services providers should be active in fulfilling their obligation of censoring the online space and be clear about the social responsibility they should bear.

5. CONCLUSION

Overall, a comparison is drawn in this study between Qvod and Winny case, based on which an analysis is conducted from the perspective of technology and management regarding the judicial boundary of Qvod Company in the case as a provider of P2P network sharing technology. Technically, the P2P+CDN model is adopted by Qvod Company to capture the hot spot videos with a high caching, view, and click counts through technology mechanisms, which is classified as passive caching. Besides, there is no criminal liability incurred to network technology provider for the spread of pornographic content. Being aware of pornographic videos in the caching server, Qvod Company acquiesces their spread through the Qvodplayer for commercial interests, rather than taking swift action against it. Despite its capability to restrict the spread of pornographic videos, Qvod Company continues allowing

users to share and request playing them repeatedly, in addition to presenting users with pornographic videos through its caching server, which is an intentional move. Thus, as the administrator, Qvod Company fails to fulfill its regulatory responsibility, incurs criminal liability. In the ever-changing time of scientific and technological development, network service providers bear the responsibility to balance the detrimental effects brought about by technical improvements to society and carry out safety management from the technical perspective proactively to safeguard society from the potential harm done by technologies to the largest extent.

REFERENCES

[1] Beijing Haidian District People's Court. (2015). *The First Instance Criminal Judgment of Wu Ming et al. on the Crime of Making, Duplicating, Publishing, Selling and Displaying Obscene Articles for Prosperity*, no. 512.

[2] Liu, Y. H. (2016). Innocent Kuaibo and Guilty Thinking-Reflection and Criticism on the Guilty Theory of Kuaibo Case. *Politics and Law, 12*, 104-113. doi: 10.15984/j.cnki.1005-9512.2016.12.011

[3] Wu, Y. C. (2017). On the Judicial Determination of Neutral Helping Acts-Comparative Analysis of Kuaibo Case and Winny Case. *Journal of Law Application, 12*, 3-10. Retrieved from https://kns.cnki.net/kcms/detail/detail.aspx?FileName=FLSS201712002&DbName=CJFQ2017

[4] Gao, L. (2017). On the Criminal Responsibility of P2P Sharing Service Provider-Taking Qvod Case as Vision. *Global Law Review, 39(5)*, 81-96. Retrieved from https://kns.cnki.net/kcms/detail/detail.aspx?FileName=WGFY201705006&DbName=CJFQ2017

[5] Fan, J. (2017). Related composition of Qvod case and related trial issues - the approach of judging behavior from technology. *Peking University Law Journal, 29(1)*, 29-50. Retrieved from https://kns.cnki.net/kcms/detail/detail.aspx?FileName=WFXZ201701004&DbName=CJFQ2017

[6] Shi, M. Y. (2017). Research on the Application of Technology Neutrality Principle in the Judgement of Copyright Infringement-P2P Streaming Media as the Research Direction. *Lanzhou University, 4*. Retrieved from https://kns.cnki.net/kcms/detail/detail.aspx?FileName=1017714590.nh&DbName=CMFD2018

[7] Chen, X. L. (2017). The judgment of the first instance of Kuaibo case is evaluated by the pedagogy of punishment law. *Peking University Law Journal, 29(1)*, 7-28. Retrieved from https://kns.cnki.net/kcms/detail/detail.aspx?FileName=WFXZ201701003&DbName=CJFQ2017

[8] Zhang, M. K. (2016, September 14). Brief analysis of conviction and sentencing in Kuaibo case. *People's Court Daily*. Retrieved from https://kns.cnki.net/kcms/detail/detail.aspx?FileName=RMFY201609140032&DbName=CCND2016

[9] Zhou, G. Q. (2017). A Study on the Reasons for Condemnation in the Case of Criminal Domination or Violation of Obligation. *Peking University of Law Journal, 1(29)*, 51-67. Retrieved from https://kns.cnki.net/kcms/detail/detail.aspx?FileName=WFXZ201701005&DbName=CJFQ2017

[10] Wu, S. K., & He, L.T. (2019). Legal identification and regulation of network cache - from the perspective of Qvod case. *Law of Finance and Economics, 5*, 41-56. doi: 10.16823/j.cnki.10-1281/d.2019.05.004

[11] CHEN, H.B. (2019). The Criminal Boundary of the Act of Technological Neutrality. *Journal of Nantong University, 1(35)*, 58-65. Retrieved from https://kns.cnki.net/kcms/detail/detail.aspx?FileName=NTSX201901009&DbName=CJFQ2019

[12] The Supreme People's Court and the Supreme People's Procuratorate. (2019). *Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues Concerning the Law Applicable to Criminal Cases of Illegal Use of Information Networks and Assisting Information Network Crimes*, no.15.

[13] Wang, H. W. (2017). The Path of Analyzing Criminal Responsibility of Internet Service Provider: With Discussion of Kuaibo Case. *Journal of National Prosecutors College, 5(5)*, 3-32. Retrieved from https://kns.cnki.net/kcms/detail/detail.aspx?FileName=ZJGX201705001&DbName=CJFQ2017