

Unfair Competition Issues of Big Data in China

*Huang-Chih Sung*¹

Abstract: The sound development of the market in the data-driven economy depends on the free and fair competition of big data in the industries. Since 2015, more and more unfair competition cases concerning big data have occurred in China, such as masking advertisement, click fraud, malicious incompatibility, and gathering user's personal data from competitors by unfair means, which can be categorized to unfair competition about illegal collection/use of competitors' big data and about network traffic. Whether China's current legal system of anti-unfair competition can resolve the above-mentioned disputes is concerned in this article. As the Paris Convention only regulates the basic principles of "fairness" and "honest practice" for anti-unfair competition, member states have room to develop their own legal systems according to their special economic, social and cultural conditions. In order to usher in the era of digital economy and big data and to regulate more and more unfair competition events, China amended the Anti-Unfair Competitive Law in 2017 in which a new provision for regulating the operation of e-commerce was added. This article finds that the 2017 Amendment, which is far more specific and clearer than the Paris Convention, has significantly improved China's ability to deal with unfair competition behaviors regarding big data. However, since the patterns of unfair competition in big data are changing and "innovating" quickly and constantly, law amendments will hardly or even never catch up with the changes, so judgement of unfair competition is inherently difficult. The court cannot determine that a company constitutes unfair competition simply because its business operations have substantially reduced the performance or operating effectiveness of its competitors. When judging whether an enterprise's competitive behavior constitutes unfair competition, no matter the court is applying one of the specific provisions or the general provision, it is essential to consider whether the enterprise has malicious and dishonest practices.

Keywords: big data, data-driven economy, unfair competition, network traffic hijacking

1 Huang-Chih Sung is Associate Professor of Graduate Institute of Technology, Innovation, and Intellectual Property Management at the National Chengchi University in Taiwan. This Article is a part of the academic performance of the research projects sponsored by Taiwan Ministry of Science and Technology (MOST 108-2410-H-004 -140 -MY2). The author is very thankful to the Taiwan Ministry of Science and Technology for its support, and solely responsible for all of the concepts and opinions in this article.

Introduction

Big data, thought as “new oil”,² is the most important driver in the data-driven economy.³ As the data-driven economy is rapidly booming, the acquisition and use of big data has become the most critical factor in corporate competition. The sound development of the market in the data-driven economy depends on the free and fair competition of big data in the industries. Accordingly, the maintenance of free and fair competition order in the big data-related market has become the most essential topic for the healthy development of the digital economy. Since the issues of restrictive competition and unfair competition derived from big data increase significantly, academic studies on the subject of competition law in the data-driven market becomes an urgent task.

The competition authorities in the globe paid attention earlier to the topics whether the collection and use of big data would raise restrictive competition or unfair competition issues. The European Data Protection Supervisor published a white paper on privacy and competitiveness in the age of big data in 2014, exploring the interaction between data protection, competition law, and consumer protection in the digital economy.⁴ In a white paper published in 2015 that explored big data growth and data-driven market innovation, the OECD pointed out that the data-driven market is much more concentrated than other markets, so the winners often take it all and obtain the dominant position of big data.⁵ The French Autorité de la concurrence and the German Bundeskartellamt jointly issued a report called “Competition Law and Data” in 2016, stating its position regarding the competition law issues of big data.⁶ Margrethe Vestager, the Executive Committee chairman of European Commission, also issued a statement in 2016, stating that the European Commission will carefully consider the

2 Perry Rotella, *Is Data the New Oil?* Forbes (Apr. 2, 2012), <https://www.forbes.com/sites/perry-rotella/2012/04/02/is-data-the-new-oil/#2bd9dcd97db3> (last visited Dec. 13, 2019).

3 Nathan Newman, *Search, Antitrust and the Economics of the Control of User Data*, 31 Yale J. on Regulation 401, 403 (2014).

4 European Data Protection Supervisor, *Privacy and Competitiveness in the Age of Bit Data: the Interplay between Data Protection, Competition Law and Consumer Protection in the Digital Economy* (2014). Available at: https://edps.europa.eu/sites/edp/files/publication/14-03-26_competition_law_big_data_ex_sum_en_0.pdf (last visited Dec. 15, 2018).

5 OECD, *White Paper, Data-Driven Innovation: Big Data for Growth and Well-Being* 7 (2014). Available at: <https://www.oecd.org/sti/inno/data-driven-innovation-interim-synthesis.pdf> (last visited Dec. 13, 2019).

6 Autorité de la concurrence & Bundeskartellamt, *Competition Law and Big Data* (2016). Available at: <http://www.autoritedelaconcurrence.fr/doc/reportcompetitionlawanddatafinal.pdf> (last visited Dec. 13, 2019).

issue of competition law for big data.⁷ Since 2017, legal academic papers have also begun to discuss competition issues on big data, including the competition policy in the data-driven economy,⁸ the entry barriers to big data,⁹ the antitrust problems and regulation of big data,¹⁰ and the interaction between IP Laws and data protection.¹¹

Since 2015, more and more unfair competition cases concerning big data have occurred in China, such as masking advertisement, click fraud, malicious incompatibility, and gathering user's personal data from competitors by unfair means. Because the types of cases and the legal system regarding anti-unfair competition in China are different from those in Western countries, none of the above issues was discussed in previous literature. This article is aiming at filling this research gap. Whether China's current legal system of anti-unfair competition can resolve the above-mentioned disputes is concerned in this article. I study the cases of unfair competition in China and explore their significances under the "Anti-Unfair Competition Law", which was amended in 2017 to cope with the unfair competition issues in the digital economy era. This article develops the theory of unfair competition issues in big data and hopes to contribute to both academic development and practical operations.

Chapter 2 of this article introduces the development history of anti-unfair competition law. From 1883 to 1958, the norms for regulating unfair competition have gradually evolved with the development of the Paris Convention, from merely declaring the general principles to slightly more specific norms. As the Paris Convention only regulates the basic principles of "fairness" and "honest practice" for anti-unfair competition, member states have room to develop their own legal systems according to their special economic, social and cultural conditions. China's Anti-Unfair Competition

-
- 7 Margrethe Vestager, Prepared Remarks, *Making Data Work for Us - Data Ethics Event on Data as Power* (Sept. 9, 2016).
- 8 Justus Haucap, *Competition and Competition Policy in a Data-Driven Economy*, 54 *Intereconomics* 201 (2019); Mira Burri, *Understanding the Implications of Big Data and Big Data Analytics for Competition Law—An Attempt for a Primer*, in Klaus Mithis & Avshalom Tor (eds), *New Developments in Competition Behavioral Law and Economics* (2018); Roberto Augusto Castellanos Pfeiffer, *Digital Economy, Big Data and Competition Law*, 3 *Market and Competition Law Review* 53, 73 (2019).
- 9 Daniel L. Rubinfeld & Michal S. Gal, *Access Barriers to Big Data*, 59 *Ariz. L. Rev.* 339 (2017).
- 10 John M. Yun, *Antitrust After Big Data*, *Baltic Yearbook of International Law* 19-24 (2019); D. Daniel Sokol & Roisin Comerford, *Antitrust and Regulating Big Data*, 23 *Geo. Mason L. Rev.* 1139 (2016); Joshua D. Wright & Elyse Dorsey, *Antitrust Analysis of Big Data*, *CLPD* 2, 35, 36 (2016).
- 11 Francesco Banterle, *The Interface Between Data Protection and IP Law: The Case of Trade Secrets and the Database sui generis Right in Marketing Operations, and the Ownership of Raw Data in Big Data Analysis*, in *Personal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach?* 411, 422 (2018).

Law enacted in 1993 is then introduced and analyzed. In 1996, the international bureau of World Intellectual Property Organization (WIPO) released the “Model Provisions on Protection Against Unfair Competition” to further implement the obligation for member states of Paris Convention Union to provide protection against unfair competition. However, the aforementioned regulations were all formulated before the development of the digital economy. In order to usher in the era of digital economy and big data and to regulate more and more unfair competition events, China amended the Anti-Unfair Competitive Law in 2017 in which a new provision for regulating the operation of e-commerce was added. Whether they can be used to regulate the fair competition of big data is an essential legal issue that must be faced.

The unfair competition behaviors regarding big data in China can be divided into two categories: unfair competition about illegal collection and use of competitors’ big data and about network traffic. Unfair competition about illegal collection and use of competitors’ big data are explained and analyzed in Chapter 3, and Unfair competition about network traffic is explained and analyzed in Chapter 4.

Development History of Anti-Unfair Competition Law

The regulation of unfair competition began in the Paris Convention in 1883. Unlike the regulations of restrictive competition that are relatively clear and focus on abuse of monopolistic position and merger applications, the concept and norms of unfair competition have always been unclear and ambiguous. As a result, it is difficult for the courts to make decisions because they lack a clear legal ground for the anti-unfair competition cases. Moreover, operators have no clear norm of conduct, such that the uncertainty and risks of business operations significantly increase. With the emergence of a variety of unfair competition practices in the era of big data, the incompleteness of the legal system of anti-unfair competition has become more apparent. To interpret the incompleteness of the legal system of anti-unfair competition, it is necessary to start with the Paris Convention.

Paris Convention: Origin of the Anti-Unfair Competition Norms

The Paris Convention, established in 1883 and amended seven times, is the first and most important international convention for the protection of industrial property rights.¹² From not only the perspectives of establishment time but also the number of member states, the Paris Convention that established many essential principles of

12 Gustavo Bravo, *From Paris Convention to TRIPs: A Brief History*, 12 *J. of Contemporary Legal Issues*, 445, 445-446 (2001).

intellectual property rights is the most representative conventions governed by the World Intellectual Property Organization (WIPO).¹³ However, the original version of the Paris Convention in 1883 did not contain any provision regarding the prohibition of unfair competition.

Until 1900, the Revision Conference of Brussels inserted Article 10*bis* to introduce the national treatment principle with respect to unfair competition.¹⁴ The current Sentence (1) of Article 10*bis*¹⁵ was introduced in the Revision Conference of Washington in 1911 by obligating all member states to assure effective protections to nationals of the countries of the Union against unfair competition.^{16, 17} However, there was no clear definition of unfair competition at that time. The concept of “unfairness” reflects the values of a particular society at a particular point in time and thus varies from country to country.¹⁸ Therefore, the definition of “unfairness” must be further clarified, otherwise the internationalized understanding and implementation of this clause cannot be reached.

The first definition of unfair competition was introduced in the Revision Conference of The Hague in 1925,¹⁹ which stipulated that any competition act contrary to honest practices in industry or commerce constitutes unfair competition.²⁰ The Revision Conference of The Hague also provided an example of unfair competition, regulating that the member states shall prohibit any activity to create confusion by any means in

13 Hans Peter Kunz-Hallstein, *The United States Proposal for a GATT Agreement on Intellectual Property and the Paris Convention for the Protection of Industrial Property*, 22 *Vanderbilt J. of Transnational L.* 265, 265-266 (1989).

14 *Actes de Bruxelles*, pp. 164 (proposal of France), 187/8, 310; 382/3 (discussions and adoption).

15 Article 10*bis* (1) of Paris Convention: “The countries of the Union are bound to assure to nationals of such countries effective protection against unfair competition”.

16 *Actes de Washington*, pp. 53 (proposal), 105, 224 (observations), 305 (report of Committee), 310 (report to Plenary Committee), 255 (discussion and adoption in Third Plenary Session).

17 Patricia V. Norton, *Effect of Article 10bis of the Paris Convention on American Unfair Competition Law*, 68 *Fordham L. Rev.* 225, 225 (1999).

18 Carlos María Correa, *Unfair Competition Under the TRIPS Agreement: Protection of Data Submitted for the Registration of Pharmaceuticals*, 3 *Chicago Journal of International Law* 69, 77 (2002).

19 *Actes de la Haye*, pp. 252/5 (proposal), 348/51 (observations), 472/8 (report of Fourth Sub-Committee), 525 (report of General Committee), 546/7 (report of Drafting Committee), 578/81 (discussion and adoption in Second Plenary Session). 1 *Actes de Londres*, pp. 197/8 (proposal), 287/90 (observations), 411/22 (report of Fourth Sub-Committee), 469/70 (report of Drafting Committee), 519 (adoption in Second Plenary Session).

20 Article 10*bis* (2) of Paris Convention: “Any act of competition contrary to honest practices in industrial or commercial matters constitutes an act of unfair competition”.

respect to the establishment, the goods, or the commercial activities of a competitor.²¹ Later, the Revision Conference of Lisbon in 1958 added two further examples of unfair competition,²² namely the acts of false allegation and misleading the public about the products or services of competitors.²³

In sum, under the Paris Convention, all member states have the obligation of assuring effective protection against unfair competition, which is defined as a competition act contrary to honest practices in industry or commerce. However, the meaning of “honest practices” is still an abstract and vague concept, and varies from country to country.²⁴ Therefore, the legal system of unfair competition is destined to be difficult to achieve international harmonization, and each country may choose its own way. Fortunately, there have been already three specific examples of unfair competition acts for countries to use for making legislation to reflect their own moral, sociological and economical principles, including creating confusion, false allegation and misleading the public about the products or services of competitors.

China’s Anti-Unfair Competition Law in 1993

Based on the Paris Convention, China enacted Anti-unfair Competition Law in 1993 (the “1993 Anti-Unfair Competition Law”). The purpose of this law was to encourage and protect fair competition, prevent acts of unfair competition, and protect the legitimate rights and interests of business operators and consumers.²⁵ The term “operators” means individuals, legal persons, and other economic organizations that are engaged in the operation of goods or for-profit services.²⁶ The term “unfair competition” refers to acts in which a business operator violates the provisions of this law, damages

21 Article 10*bis* (3.1) of Paris Convention: “The following in particular shall be prohibited: 1. all acts of such a nature as to create confusion by any means whatever with the establishment, the goods, or the industrial or commercial activities, of a competitor”.

22 *Actes de Lisbonne*, pp.725, 784 (proposal of Austria), 725/6 (discussion in Third Committee), 789/90 (discussion in Fourth Committee), 852 (report of Fourth Committee), 726/7, 790 (discussion in General Committee), 106 (adoption in Second Plenary Session), 118 (General Report).

23 Article 10*bis* (3.2) of Paris Convention: “2. false allegations in the course of trade of such a nature as to discredit the establishment, the goods, or the industrial or commercial activities, of a competitor”; Article 10*bis* (3.3) of Paris Convention: “3. indications or allegations the use of which in the course of trade is liable to mislead the public as to the nature, the manufacturing process, the characteristics, the suitability for their purpose, or the quantity, of the goods”.

24 Correa, *supra* note 17, at 81.

25 Article 1 of the 1993 Anti-unfair Competition Law.

26 Article 2(3) of the 1993 Anti-unfair Competition Law.

the legitimate rights and interests of other operators, and disrupts the social and economic order.²⁷

The 1993 Anti-Unfair Competition Law stipulated some regulations regarding trademark and authentication mark infringements,²⁸ trade secret infringements,²⁹ bribery and off-the-book rebate,³⁰ misleading or false advertising,³¹ and lottery-attached sale activities.³² Nevertheless, since it was developed much earlier than the development of the digital economy, the 1993 Anti-Unfair Competition Law did not specifically regulate any acts of unfair competition related to big data. For the unfair competition issues regarding big data, this law only provided the basic principles of anti-unfair competition on the ground of the Paris Convention, stipulating that operators in market transactions should follow the principles of voluntariness, equality, fairness, and honesty, and observe the generally accepted business ethics.³³ As a result, while adjudicating the cases concerning unfair competition, China's courts could only expansionary interpret such general principles as the legal basis for their judgments.³⁴ On the one hand, it was difficult for the courts to make decisions because they lacked a clear legal ground for the anti-unfair competition cases. On the other hand, operators did not have a clear norm of conduct, such that the uncertainty and risks of business operations significantly increased. In the era of the digital-driven economy, this law was more inadequate to regulate the unfair competition acts related to big data collections and uses.

The WIPO Model Provisions in 1996

In order to provide a standard for member states to implement protection against unfair competition on the ground of Article 10*bis* of the Paris Convention,³⁵ the international bureau of WIPO released "Model Provisions on Protection Against Unfair

27 Article 2(2) of the 1993 Anti-unfair Competition Law.

28 Article 5 of the 1993 Anti-unfair Competition Law.

29 Article 10 of the 1993 Anti-unfair Competition Law.

30 Article 8 of the 1993 Anti-unfair Competition Law.

31 Article 9 of the 1993 Anti-unfair Competition Law.

32 Article 13 of the 1993 Anti-unfair Competition Law.

33 Article 2(1) of the 1993 Anti-unfair Competition Law.

34 See Lanfang Fei & Peng Zhou, *Technological Interference, Public Interest and Unfair Competition – A Critical Review of China's Practice*, 48 IIC-International Review of Intellectual Property and Competition Law 436, 439 (2017).

35 Marcus Höpferger & Martin Sentleben, *Protection Against Unfair Competition at the International Level – The Paris Convention, the 1996 Model Provisions and the Current Work of the World Intellectual Property Organisation*, in Reto M. Hilty & Frauke Henning-Bodewig (eds.), *Law Against Unfair Competition-Towards a New Paradigm in Europe?* 61, 72 (2019).

Competition” (hereinafter the “WIPO Model Provisions”) in 1996, which further implemented the obligation for member states of Paris Convention Union to provide for protection against unfair competition.³⁶ WIPO specifically regulates five acts of unfair competition, namely: (1) causing confusion with respect to another’s enterprise or its activities; (2) damaging another’s goodwill or reputation; (3) misleading the public; (4) discrediting another’s enterprise or its activities; (5) unfair competition in respect of secret information. The first two are related to the protection of trademark or goodwill, and the last one is regarding the protection of trade secret, all of which are not relevant to big data and thus beyond the scope of this article.

Under Article 4 of the WIPO Model Provisions, any act during commercial activities that misleads the public in respect of the products or services offered by another’s enterprise constitutes unfair competition.³⁷ It also lists some types of misleading activities that may arise out of promotion or advertising, such as misleading the quality, quantity, or conditions of the products or services provided by the competitors.³⁸ Article 5 of the WIPO Model Provisions stipulates that any unjustifiable or false allegation during commercial activities that discredits the products or services offered by another’s enterprise constitutes unfair competition.³⁹ Some types of discrediting activities are also listed that may arise out of promotion or advertising, such as misleading the quality, quantity, or conditions of the products or services provided by the competitors.⁴⁰ Both provisions may apply to unfair competition issues regarding big data, especially advertising-related behaviors.

The greatest contribution of the WIPO Model Provisions is to list five behaviors that may constitute unfair competition together with examples. However, the WIPO Model Provisions are neither an international treaty nor a soft law, so they have no legal binding on governments in the world.⁴¹ Instead, they are only a reference for court decisions and a model for legislative activities.⁴² Furthermore, these regulations are still not specific enough, and need to be interpreted and supplemented by competition authorities and courts of various countries. Especially, all of the aforementioned regulations were enacted before the development of data-driven economy. Whether they

36 Notes on Article 1 of the WIPO Model Provisions.

37 Article 4(1) of the WIPO Model Provisions.

38 Article 4(2) of the WIPO Model Provisions.

39 Article 5(1) of the WIPO Model Provisions.

40 Article 5(2) of the WIPO Model Provisions.

41 Höpperger & Senftleben, *supra* note 34, at 83.

42 *Id.*

can be suitably applied to regulate the fair competition order of big data is an essential legal issue to be studied.

2017 Amendment of Anti-Unfair Competitive Law

As mentioned, the Paris Convention only regulates the basic principles of “fairness” and “honest practice” for anti-unfair competition, leaving countries with room to develop their own legal systems according to their special economic, social and cultural conditions. In order to usher in the era of digital economy and big data and to regulate more and more unfair competition events, China amended the Anti-Unfair Competitive Law in 2017 (“2017 Amendment”), in which a new provision for regulating the operation of e-commerce was added. Article 12 of the 2017 Amendment stipulates that any business operator who conducts business activities on the Internet shall follow the Anti-Unfair Competitive Law. They shall not use any technical measures to influence Internet users’ choices to perform the following acts that could hinder or disrupt the normal operation of online products or services provided by other operators: (1) without the consent of other e-business operators, inserting links and forcibly performing target jumps in the network products or services they legally provide; (2) deceiving, misleading, or forcing users to modify, shut down, or uninstall online products or services legally provided by other e-business operators; (3) malicious implementation of incompatible online products or services legally provided by other e-business operators; (4) other acts that obstruct or disrupt the normal operation of online products or services provided by other e-business operators.

This new law amendment specifically lists four types of unfair competition acts that often occur in China in the era of e-commerce. This article will discuss whether these new regulations will help solve China’s problems of unfair competition in big data.

Illegal Collection and Use of Competitors’ Big Data

Unfair Competition Caused by Illegally Collecting Competitors’ Big Data

A company may constitute unfair competition if it uses unfair and illegal technical means to crawl data on the websites of competitors without their consents and then uses it for its own goods or services for competition or business transactions in an apparently unfair manner. *Weimeng v. Taoyou*⁴³ is the first case in China that a company was held in violation of the Anti-Unfair Competition Law by illegally grabbing competitor’s big data.

43 Weimeng v. Taoyou, 2016 Judgement No. 588 of Beijing 73 Min Zhong (2016).

Sina Weibo, operated by Beijing Weimeng Chuangke Network Technology Co., Ltd. (hereinafter “Weimeng”), is a large microblogging website in China. Weimeng filed a lawsuit against the defendant companies (Beijing Taoyou Tianxia Technology Development Co., Ltd. and Beijing Taoyou Tianxia Technology Co., Ltd.; collectively “Taoyou”) in Beijing Haidian District Court in 2016, claiming that the social media MeiMei operated by the defendants Taoyou constituted unfair competition by using illegal means to capture the user profiles of its members.⁴⁴ After adjudication, the court held that the defendants had violated the Anti-Unfair Competition Law so they should stop conducting unfair competition behavior and compensate the plaintiff for damages.⁴⁵ The defendants appealed to the Beijing Intellectual Property Court. The Beijing Intellectual Property Court found that Taoyou had captured the user profiles of non-MeiMei’s Weibo members without the approval of Weimeng.⁴⁶ The Beijing Intellectual Property Court thus dismissed the appeal in December 2016, holding that the defendants did not only constitute unfair competition but also violate the principle of good faith and the business ethics of e-commerce.⁴⁷

In details, Weimeng operates Sina Weibo, which is both a social media network platform and an open platform for providing interfaces to third-party applications. MeiMei, the software provided by the defendants, is a mobile social application software. Since Taoyou signed a cooperation agreement with Weimeng in the beginning stage, the users could register MeiMei by using their Sina Weibo’s accounts and mobile phone numbers. When a user was registering a MeiMei account, he also needed to upload the contact list in his mobile phone. Due to Sina Weibo’s poor management of the Open Application Programming Interface (Open API), Taoyou could capture the personal data of its members without the authorization of Sina Weibo, including name, occupation, and education level. Since the defendants had owned the contact lists in MeiMei user’s mobile phones, they could discover non-MeiMei’s Weibo members by finding the mobile phone numbers in the contact list of MeiMei’s users and then identify the non-MeiMei’s Weibo members by indexing the mobile phone numbers to Weibo’s database. Taoyou then captured the personal data of the non-MeiMei’s Weibo members without the approvals of the members and Sina Weibo.⁴⁸ The court thus noted that Taoyou’s behaviors endangered the information security of the Sina Weibo platform

44 *Id.*

45 *Id.*

46 *Id.*

47 *Id.*

48 *Id.*

and harmed the legitimate competitive interests of Weimeng Company.⁴⁹ Therefore, the Beijing Intellectual Property Court concluded that Taoyou's illegal scrawling of Sina Weibo's data had constituted unfair competition and must compensate Weimeng for its economic loss.⁵⁰

Unfair Competition Caused by Illegally Using Competitors' Big Data

After the cooperation between Weimeng and Taoyou had been terminated, Taoyou did not delete the avatar, name, occupation, education, and personal tags of Sina Weibo's users obtained from Weimeng in time but continued to use them. The Beijing Intellectual Property Court in the *Weimeng v. Taoyou* case also held that Taoyou's illegal use of Sina Weibo's data not only endangered the cyber security of Sina Weibo's users on the platform, but also damaged the legitimate competition interests of Weimeng.⁵¹ Therefore, the Beijing Intellectual Property Court concluded that Taoyou's illegal use of Sina Weibo's data had also constituted unfair competition and must compensate Weimeng for its economic loss.⁵²

Analysis

Without the consent of data owners, the behavior of hacking into other's websites or databases to illegally crawl and use data is becoming more frequent. Illegal crawling and use of other's data may not only endanger the personal data privacy of the data subjects, but also damage the legitimate competition interests of the owner of the websites or databases. Such conducts are indeed "unfair" and "dishonest practice" under the Paris Convention. Since big data usually cannot be protected by the traditional intellectual property rights, Anti-Unfair Competition Law may become the last mechanism for data owners to protect their interests and claim damages. However, these two behaviors do not suffice the four types of unfair competition acts regulated by China's 2017 Amendment of Anti-Unfair Competitive Law. Therefore, the court can only apply the general provisions of Article 2 as the basis for judgment.

In addition to civil liability, the defendants in the aforementioned case may also commit a crime of trespassing to computer information systems under Article 285 of the Chinese Criminal Law, in which the behavior of hacking into others' computer systems to obtain data stored, processed or transmitted in the computer systems could be punished by imprisonment for up to three years. In the European Union and America,

49 *Id.*

50 *Id.*

51 *Id.*

52 *Id.*

such conducts are also punishable by criminal law. For example, Directive 2013/40/EU on attacks against information systems establishes regulations concerning the definition of sanctions and criminal offences in the field of attacks against information system.⁵³ Intentionally illegal access to other's information system without permission is punishable as a criminal offence under Directive 2013/40/EU.⁵⁴ Moreover, Computer Fraud and Abuse Act of the United States (18 U.S.C. § 1030), an amendment to previous Computer Fraud Law, was enacted in 1986 to establish rules to punish frauds and related activities in connection with computers.⁵⁵ Under the Computer Fraud and Abuse Act, whoever with knowingly accessed other's computer without or exceeding authorization is punishable as a criminal offence.⁵⁶ However, the constitution of a criminal offense is premised on the "knowingly and with intent" of the defendant. It is generally not easy for the prosecutor to prove that. Therefore, the use of anti-unfair competition law to resolve such disputes from civil liability still has its significance and value.

Unfair Competition about Network Traffic

The unfair competition behaviors regarding network traffic can be divided into two categories: unfair competition caused by click fraud and by network traffic hijacking.

Unfair Competition Caused by Click Fraud

In the data-driven market, pay-per-click is the mostly used mode for advertisement release on the web. Accordingly, web traffic⁵⁷ and online advertising clicks⁵⁸ are important indicators of webpage management. For the operators of webpages such as blogs and live videos, the greater the number of clicks, the more attractive it is for the advertisers to release advertisements and the greater the incomes they receive.

53 Article 1 of the Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (hereinafter "Directive 2013/40/EU").

54 Article 3 of the Directive 2013/40/EU.

55 18 U.S.C. § 1030. Fraud and related activity in connection with computers.

56 Article 1 of 18 U.S.C. § 1030.

57 Radovan MadleĚáka, Lucia MadleĚáková, Libor Madleňák & Daniel Salava, *Analysis of website traffic dependence on use of selected internet marketing tools*, 23 *Procedia economics and finance* 123, 124 (2015).

58 Yu (Jeffrey) Hu, Jiwoong Shin & Zhulei Tang, *Incentive Problems in Performance-Based Online Advertising Pricing: Cost per Click vs. Cost per Action*, 62 *Management Science* 2022, 2022 (2016).

The platform operators run the data-driven market based on data such as the network IP address of the Internet readers, the number of webpage's clicks, and the time of reader's stay. On the one hand, they recommend the best websites and web contents to the network readers, and on the other hand, they provide the click number of each website to the advertisers as an important basis to release advertisements and calculate the advertising fee. Therefore, the real and correct click number of each website is essential for both platform operators and advertisers.

Because the number of clicks are almost equivalent to revenue, some businesses use unfair means to help webpage operators or content providers fraudulently click the webpages, including the creation of many fake accounts and constant change of the network IP addresses. Click fraud is an active deception for both advertisers and platform operators. It may not only damage the rights of advertisers, but also affect the competition order of the digital-driven market so as to constitute unfair competition.

Beijing iQiYi Technology (hereinafter "iQiYi") is the largest video service provider in China. iQiYi found in 2017 that the number of clicks on several videos had increased abnormally. After tracing the source of the abnormal visits, iQiYi found that the defendants were engaged in the click-farming services for their clients. iQiYi filed a lawsuit against the defendant company and its representatives in Shanghai Xuhui Court in early 2018, claiming that the defendants constituted unfair competition by maliciously increasing the number of clicks on certain websites to obtain illegitimate interests from iQiYi's website.⁵⁹

In details, the plaintiff iQiYi's website provides lots of licensed videos and channels. By paying a fee monthly or annually, its members can watch all of the videos on iQiYi's website. For each video, on the one hand, iQiYi pays licensing fee to the copyright owner based on the number of times the video is watched. On the other hand, advertisers pay iQiYi for advertising also based on the number of times the video is watched.⁶⁰ Therefore, correctly calculating the number of times that each movie is viewed is the most fundamental and important task in the business of iQiYi. In addition to helping video providers and advertisers decide the cooperation modes with iQiYi, these traffic data also enable iQiYi accurately evaluate the popularity of each video and analyze the watching hobbies and time period of members from different regions, so as to make business decisions about video procurements and advertising cooperation.⁶¹

59 iQiYi v. Feiyi, 2017 Shanghai District Court 0104 Civil Judgment No. 18960 (2017).

60 *Id.*

61 *Id.*

The defendant Hangzhou Feiyi Information Technology Co., Ltd. (hereinafter “Feiyi Information”) was providing click-farming service to assist increasing video visits and enhancing video popularity.⁶² According to the court’s decision, Feiyi Information helped its clients visit iQiYi’s website to rapidly increase the number of views of some specific videos in a short period of time by continuously changing IP addresses through multiple domain names. The price is 15 RMB per 10,000 times of views. From February 1st to June 1st, Feiyi Information made at least 950 million false visits on the iQiYi website, and illegally benefited about one million RMB. iQiYi claimed for damages of RMB 5 million.⁶³

After adjudication, the Shanghai Xuhui District Court held that the defendants’ excessive increase in the number of clicks on certain webpages was not only in violation of the competition order of the relevant market, but also harmed the interests of iQiYi and its consumers.⁶⁴ For iQiYi, the false number of video visits caused it to pay more copyright license fees to the video providers, and to make incorrect business decisions which resulted in the loss of competitive advantage.⁶⁵ For consumers, the video ranking derived from false number of visits did not truly reflect their needs. The misled consumers might have bad user experiences and no longer trust the business reputation of iQiYi, so as to choose other service providers and cause the loss of the economic interests of iQiYi.⁶⁶ Shanghai Xuhui District Court thus concluded that the defendants constituted unfair competition and should jointly compensate iQiYi for RMB 500,000.⁶⁷

Both plaintiff and defendants appealed to Shanghai Intellectual Property Court. iQiYi claimed that RMB 500,000 were insufficient to compensate its loss and far lower than the benefits obtained by the defendants. The defendants asserted that the click-farming service had never damaged the legal rights of iQiYi.⁶⁸ The Shanghai Intellectual Property Court held that the act of false video clicks had substantially increased the customers’ false perceptions of the quality and popularity of the falsified videos and thus belonged to a “false propaganda” as regulated by the Anti-Unfair Competition Law.⁶⁹ For iQiYi’s request, the court held that it had already had technical means to

62 *Id.*

63 *Id.*

64 *Id.*

65 *Id.*

66 *Id.*

67 *Id.*

68 *iQiYi v. Feiyi*, 2019 Shanghai Intellectual Property Court 73 Civil Final Judgment No. 4 (2017).

69 *Id.*

block some of the fictional video clicks, so the damages were not as severe as it claimed. Therefore, the Shanghai Intellectual Property Court rejected the appeals of both parties and upheld the original judgment.⁷⁰

Unfair Competition Caused by Network Traffic Hijacking

The so-called traffic hijacking refers to the use of malicious computer programs to control and change the online behavior of innocent users, so that they open different pages than originally expected, install apps that are different from the original expectations, or see advertisements that they do not want to see. There are many kinds of behaviors in traffic hijacking, wherein DNS hijacking is the most common one.

Each node on the Internet is given an IP address to facilitate the transmission of network information and data.⁷¹ Internet users who want to browse information on a website must open a web browser to connect to the IP address of the website. However, because the IP Address is a long string of numbers, such as 168.95.192.1, it is nearly impossible for users to memorize. Accordingly, the concept of domain name was invented and some domain service providers (DSPs), such as Amazon and Google, provide a correspondence table between the domain names and IP addresses. As long as the user enters the domain name of a website, the Internet service provider (ISP) will send a request to DSP to request the corresponding IP address of the website, so that the ISP can direct the user to the website.⁷² DNS hijacking means a hacker's invasion of the DNS relay to change the DNS settings, to correspond the domain name of a target website to a specific IP address other than that of the target website.⁷³ Accordingly, when a user searches the target website by using its domain name, the hacked DSP will provide a wrong IP address and thus direct the user to a wrong website.⁷⁴

The Shanghai Pudong New District Court made a criminal verdict in 2015, which is the first verdict on traffic hijacking in China.⁷⁵ The defendants used malicious code to

70 *Id.*

71 Asam Ali Zare Hudaib, *DNS Advanced Attacks and Analysis*, 8 *International Journal of Computer Science and Security* 63, 64 (2014).

72 Sameena Naaz & Firdoos Ahmad Badroo, *Investigating DHCP and DNS Protocols Using Wireshark*, 18 *IOSR Journal of Computer Engineering* 1, 1 (2016).

73 Hudaib, *supra* note 65, at 67-68.

74 Nikolaos Alexiou, Stylianos Basagiannis, Panagiotis Katsaros, Tushar Deshpande & Scott A. Smolka, *Formal Analysis of the Kaminsky DNS Cache-Poisoning Attack Using Probabilistic Model Checking*, 2010 *IEEE 12th International Symposium on High Assurance systems Engineering*, 94, 94 (2010).

75 2345.com v. 5w.com, Shanghai Pudong New District Court (2015).

tamper with the DNS settings of Internet user routers from 2013 to 2014, so that when users log in to the portal site “2345.com”, they will be automatically directed to the unexpected portal site “5w.com”. The defendants then sold the acquired Internet user traffic to their client “5w.com” and made an illegal profit of about RMB 750,000.⁷⁶ The defendants were sentenced to three years in prison because the Shanghai Pudong New District Court held that the behavior of the defendants of modifying the data stored in the computer information system was to constitute a crime of damaging the computer information system.⁷⁷

Analysis

For the *iQiYi v. Feiyi* case, the Shanghai Intellectual Property Court made the decision in 2019, so it seems that the 2017 Amendment should be adopted as legal ground for judgment. However, since *iQiYi* filed the lawsuit prior to the effective date of the 2017 amendment (January 1, 2018), the Shanghai Intellectual Property Court still needed to make the judgment on the ground of the general provision of the 1993 Anti-Unfair Competition Law. In this case, because *Feiyi* assisted its client to fraudulently click some webpages to defraud advertising fees, it may have also constituted a criminal fraud.⁷⁸ Therefore, it is reasonable for the Shanghai Intellectual Property Court to hold that the act of false video clicks has substantially increased the customers’ false perceptions of the quality and popularity of the falsified videos and thus belonged to a “false propaganda” as being regulated by the Anti-Unfair Competition Law. If there are similar cases in the future, the courts can adopt the fourth sentence of the 2017 Amendment to make judgments. From this perspective, the 2017 Amendment has significantly improved the maturity of China’s legal system of anti-unfair competition.

In addition to criminal responsibility, DNS hijacking may cause great damages to users. For instance, a user originally wants to visit Website A, but is directed to Website B because of an illegal DNS hijacking. If the user interface of Website B is very similar to Website A, the user may mistakenly believe that Website B is Website A, and thus enters his account number, password, or other personal data such as credit card number, resulting in important personal information being illegally obtained by Website B. In addition, DNS hijacking may also cause great damages to website operators. For instance, the aforementioned user originally expects to visit Website A, but is directed to Website B by an unlawful DNS hijacking. Website A would lose the network traffic that it could originally obtain, thereby losing the business opportunities or advertising

76 *Id.*

77 *Id.*

78 Article 266 of China’s Criminal Law.

benefits that it might have obtained. Therefore, DNS hijacking may also constitute unfair competition for websites that have been hijacked. If there are similar cases in the future, the courts can adopt the first sentence of the 2017 Amendment to make judgments. This confirms again that the 2017 Amendment, which is far more specific and clearer than the Paris Convention, has significantly improved China's ability to deal with unfair competition behaviors regarding big data.

However, since the patterns of unfair competition in big data era are changing and "innovating" quickly and constantly, law amendments will hardly or even never catch up with the changes. For this reason, it is inherently difficult for the courts to judge unfair competition cases. Based on the spirit and principles of the Paris Convention, this article suggests that a company should not be held unfair competition simply because its business operations have substantially reduced the performance or operating effectiveness of its competitors. When judging whether a company's competitive conduct constitutes unfair competition, no matter the court is applying one of the specific provisions or the general provision, it is essential to consider whether the company has malicious and dishonest practices and whether its behavior harms the consumers and market competition order.

Conclusion

As the data-driven economy is rapidly booming, the collection and use of big data have become the most essential factor in company competition. The sound development of the market in the data-driven economy depends on the free and fair competition among the industries. Since 2015, more and more unfair competition cases concerning big data have occurred in China, such as masking advertisement, click fraud, malicious incompatibility, and gathering user's personal data from competitors by unfair means. This article categorizes them into unfair competition about illegal collection/use of competitors' big data and about network traffic fraud. Whether China's current legal system of anti-unfair competition can resolve the above-mentioned disputes is concerned in this article.

As the Paris Convention only regulates the basic principles of "fairness" and "honest practice" for anti-unfair competition, countries have room to develop their own legal systems according to their special social, economic, and cultural conditions. Based on the Paris Convention, China enacted the Anti-Unfair Competition Law in 1993. Since it was developed much earlier than the development of the digital economy, the 1993 Anti-Unfair Competition Law did not specifically regulate any acts of unfair

competition related to big data or e-commerce. For the unfair competition issues regarding big data, this law only provided the basic principles of anti-unfair competition on the ground of the Paris Convention, stipulating that operators in market transactions should follow the principles of voluntariness, equality, fairness, and honesty, and observe the generally accepted business ethics. As a result, while adjudicating the cases concerning unfair competition, China's courts could only provide expansionary interpretation of such general principles as the legal basis for their judgments.

In order to promote the progress of data-driven economy and to regulate more and more unfair competition events, China amended the Anti-Unfair Competitive Law in 2017 in which a new provision with four sentences was added for regulating the operation of e-commerce. The unfair competition caused by network traffic hijacking could be regulated by the first sentence. Other unfair competition behaviors such as unfair competition caused by click fraud and by illegal collection/use of Competitors' big data can be handled by the general clauses of the fourth sentence. This article finds that the 2017 Amendment, which is far more specific and clearer than the Paris Convention, has significantly enhanced China's ability to deal with unfair competition behaviors regarding big data.

However, since the conducts of unfair competition in big data are changing quickly and constantly, law amendments will hardly or even never catch up with the changes, so judgement of unfair competition cases is inherently difficult to the courts. Based on the principles raised in the Paris Convention, this article finds that the courts should not determine a company constituting unfair competition simply because its business operations have substantially reduced the performance or operating effectiveness of its competitors. When judging whether an enterprise's competitive behavior constitutes unfair competition, it is essential to consider whether the enterprise has malicious and dishonest practices and whether its behavior harms the consumers and market competition order.