1. **Overview**

The recent cases concerning privacy protection and data-related unfair competition in China touch upon a wide variety of novel and yet controversial issues from point of law. On the one hand, the passing of China Cybersecurity Law (“CSL”) and its implementing regulations (though some of them are still in the pipeline) are expected to create a comprehensive regulatory framework for cybersecurity, data compliance and privacy protection. On the other hand, increasingly active public and private enforcements show that views differ greatly on how to interpret and apply the law to various business contexts, in particular in the TMT sector.

In the present TMT series, we would like to focus on the private enforcement in China and introduce to you a number of relevant cases. Not all the cases are brought under the new law, and some of them under the Anti-unfair Competition Law (the “AUCL”), which well exemplify the complexity privacy and data protection and its interaction with other areas of law.

Looking into those cases has practical importance – they provide useful reference to help interpret and apply the law in the commercial reality. The decisions may have far-reaching impact on shaping the boundary of data related practices in all sectors of economy.

2. **Recent Cases**

2.1 *Ren Jiayu v. Baidu* (2015) – the first “right to be forgotten” case under the PRC law

The claimant was a professional adviser in human resources and management consultancy, and worked with Wuxi Taoshi Education Co., Ltd in 2014. The employment was terminated in the end of 2014. Later on, the claimant found search results on Baidu (an internet search engine) containing expressions of “Wuxi Taoshi Ren Jiayu” and other similar headings. Wuxi Taoshi’s marketing strategy was controversial, and there were allegations of dishonest and fraudulent practices against the company. Ren claimed that his reputation and right to personality were infringed by those search results as potential employers and business partners would probably associate the search results with negative perception when judging his credentials and reputation.

Although the case pre-dates the enactment of CSL (effective on June 1, 2017), its rationale remains applicable in the post-CSL period.
CSL only grants a data subject the right to request erasure of personal data in the cases of unlawful collection or in violation of privacy policy. In other words, it does not provide for a general right of erasure for the data subject. If only referring to CSL, the outcome of the case should have been the same even if it is filed after June 1, 2017.

Therefore, the key issue before the court is to examine whether the “right to be forgotten” can be framed under other causes of action, as in the present case under the notion of the right to personality.

The court went on to elaborate on the principles to be applied when analyzing the claim under the right to personality – the justification and necessity of protection. One might tend to read from the literal meaning and come up with a feeling that the principle can be interpreted to generate a comprehensive right to erasure for individuals concerned. However, the court’s interpretation suggests the contrary. It appears that the court recognized the relative nature of the right to erasure, and hence it would conduct a balanced exercise in weighing the individual’s right against information right of others and freedom of expression. The general tenor of the analysis may have implied that unless the individual’s right overwhelms other rights in a given situation, there would be no good reason to hold that why the individual’s right should be given priority over the other. Hence, the circumstances under which the personality right as an alternative to frame a “right to be forgotten” claim would be severely limited.

2.2 Sina Weibo v. Maimai (2016) – the first unfair competition case concerning big data analytics

Maimai (a career and social networking start-up) entered into a Developer Agreement (Open API) with Sina Weibo (a leading micro-blogging platform). The key arrangements under the Developer Agreement: (i) Maimai enabled Weibo’s social login function on Maimai’s webpage and mobile application, (ii) Maimai would have access to richer user profile on Weibo, and (iii) Maimai needed to follow certain rules and restrictions on collection and use of Weibo’s data. Weibo later found unauthorized collection of users’ educational and occupational information by Maimai. The central issue for the court to decide was whether the alleged “unauthorized collection and use of data” and its related activities constitute unfair competition under the AUCL.

The case is a landmark decision to address one of the important questions on competition for data resources in the internet industry: to what extent data scraping (both personal data and other data) targeting a competitor could be potentially caught by the rules of unfair competition.
There are already ample commentaries on the case and its ramifications, and here we would just like to offer some of our observations:

(a) The ownership and property right in user data

The discussion and debate over the ownership and property right in user data is a puzzle that has haunted both the internet industry and the legal profession for a long time. The first hurdle lies in the difficulty in defining the meaning of “user data” – personal data, derivative data, and other data.

The court addressed the question from the perspective of competition law instead of tackling directly the thorny issue of property right in data. The main thrust of the court’s reasoning is that Weibo invests time, manpower and other resources in collecting and maintaining its user database, the aggregation of user data would help attract more users and further increase Weibo’s online traffic. All of these make up competitive resources for Weibo, which is sufficient to bring the case under the cause of action of unfair competition. In other words, the uncertainty surrounding the ownership and property right in user data is not a bar to seeking remedies under the AUCL.

(b) the “triple authorization” principle

The court also establishes the “triple authorization” principle for collecting the user’s personal data in the open API context. Specifically, “triple authorization” principle means (i) user’s consent to the platform (ii) the platform’s authorization to a third-party service provider (iii) user’s consent directly to the platform’s service provider.

The “triple authorization” principle no doubt gives users more control over their personal data. However, the principle itself is not without controversy. The application scope of the principle and how Article 41 of CSL should be construed in light of the principle are of primary concerns to businesses. Some astute comments point out that whether indirect consent from users (as in the case of SDK developer) could be held as invalid. Another point is how the restrictive principle might affect a broad consent given by users to cover both the platform and its service providers.

(c) the rule of evidence concerning new data analytical technologies

Assuming that an internet platform discovers its user data being inappropriately collected and used by a third party and then files a complaint with the court, then how to adduce evidence to substantiate its claims becomes a key issue. This is also a practical question as the processing of such an intangible property as data requires some record and metadata to evidence and visualize the process, probably log files and
expert evidence to facilitate the court’s understanding about how the technology works. It is important to point out that the burden of proof remains with the claimant under the PRC law, as shown in the present case how the court decides based on preponderance of the evidence as to the use of collaborative filtering algorithms in Maimai’s recommender system.

2.3 *Hantao v. Baidu* (2016) – data scraping case concerning UGC (user generated content)

The case follows a similar line of reasoning. Hantao operates dianping.com, a city living guide offering promotional information and consumer reviews on catering, leisure and entertainment. Baidu, in addition to its search service, also runs its own online map. Baidu used web spider to collect consumer reviews on dianping.com and integrate them into Baidu’s online map product. Two particulars of the fact need to be highlighted: first, the UGC on dianping.com was displayed in full on Baidu’s online map; and second, the robots.txt on dianping.com did not prohibit web spiders from scraping information available on the web pages.

In addition to the similarities in terms of reasoning, we would also like to draw the following points to your attention:

(a) when analyzing if two businesses are competitors, the court will look at and compare the core functions of the products or services at issue. This is a flexible approach, which, in our view, is also the correct method. For example, in the present case, the parties were found to be in a competitive relationship because location-based services are at the core of the respective products.

(b) the court would assess the behaviors of data collection and its subsequent uses separately. In the present case, the fact that the robots.txt on dianping.com did not prohibit web crawling could not be interpreted to mean that there is not restriction on the subsequent use of the UGC. During analyzing the subsequent use of the UGC, the court adopted a similar “rule of reason” approach to weighing the pro-competitive effect against the anti-competitive effect while also taking into account of consumer welfare.

(c) in fact, the line is not easy to draw between lawful and unlawful data crawling in the context of competition. One interesting hypothetical question to put forward is: assuming a business is found to have scraped the UGC on a web site containing consumer reviews, but the business does not display the UGC directly on its own products. Instead, the business invests significantly to carry out further data analysis and use those work products on its own products, would the case be decided differently? Also,
if a platform holding a vast amount of UGC is in a dominant market position and prevent others from collecting and using its UGC, would it be possible to make a case under the Anti-monopoly Law? Perhaps it would not be too long to see how the courts would consider those challenging questions.

2.4  *Tencent v. Douyin (2019)* – the debate over the ownership of users’ ID, nicknames and profile pictures

The fact of the case bears a close resemblance to the Maimai case. Douyin had entered into a Developer Agreement with WeChat and QQ platforms, and had access to users’ WeChat and QQ IDs, nicknames and profile pictures. Douyin had shared those data with Duoshan, a social networking product run by its affiliate. WeChat and QQ platforms claimed that the unauthorized use of IDs, nicknames and profile pictures of their users constitute unfair competition. The court granted a temporary injunction restraining Douyin from using those user data until the date of final judgment. It remains to be seen whether the court would consider the case following the same logic of the Maimai case.

3.  **Key Takeaways**

In this Key Takeaways section, we would shift our focus from case analysis to our observations as well as their practical implications for clients.

- Based on the identity of the claimant and the counterparty, the above cases can be divided into two categories: (i) between consumer and internet service provider, and (ii) between businesses. The former category is centered around the limit of the data subject’s rights, while the latter focuses on where the line between fair and unfair competition involving data collection and use should be drawn.

- In the first category, the consumer’s rights in the capacity as data subject would naturally turn to a compliance obligation for the business. For example, if “the right to be forgotten” is broadly construed under the PRC law, a company defined as network operator would then need to invest additional resources and IT upgrading to handle related requests.

- The importance of the second category lies in the fact various business activities involving data collection and use might now be subject to new dimensions of regulations (i.e. unfair competition, data ownership and data use right). The conventional approach is to invoke protection under trade secrets rules and contractual damages. However, the ambiguity in ownership of UGC makes it inapt to rely invariably on the conventional approach. Likewise, the use of internet bots in crawling, scrapping and parsing data which is the possession of other businesses also poses challenging situations – to what extent it should be allowed to encourage innovation and to what extent prohibited to regulate unfair competition. The line
in between is becoming increasingly blurred and the rule of reason approach may also suggest that the outcome would be less predictable.

- Currently, it appears that Article 2 of the AUCL is the main battleground of unauthorized data scrapping and data uses among internet platforms, but this does not imply that it is a cause of action that can be easily relied upon. The advantage of Article 2 is largely attributed to the fluid nature of its wording so that it could be potentially applicable to all kinds of data practices. This, however, by no means guarantees a satisfactory outcome and considerable uncertainties remain as to how the court may decide. This is because the court will need to carry out a balanced exercise to assess the overall impact of its decision to market competition. Most importantly, the court expressed its attitude of judicial prudence when intervening in business models containing the elements of novel technology and data analytics. The attitude may well point to a direction where it would not be realistic to invoke Article 2 to prevent all kinds of data scraping activities and “free rider” problems.

- When it comes to the customer-facing side of the analysis, the compliance obligations of businesses are comprised of (i) information security obligations via-a-vis IT system, configurations, and personal data storage and transfer, and (ii) response to the data subject’s rights. We observe that the relevant statutory provisions so far have granted limited rights to a data subject, and the courts have generally adopted a cautious approach to privacy cases. Combining the two factors, the overall compliance burden of businesses in China is still largely focused on the cybersecurity aspect.

- Perhaps it would be interesting to further point out that the relevant cases up to date have been filed under the AUCL instead of the Anti-Monopoly Law of China (the “AML”). And perhaps it would not be long before the first case to test how data related competition behaviors should be reasoned under the AML. The challenges at first sight would be the definition of the relevant market given the inherent fluid nature of the term “data” and its subsequent use, but enforcement actions and cases in other jurisdictions may shed some light on whether or not similar arguments may be accepted before the Chinese courts, which, albeit challenging, is not a mission impossible.

- Last but not least, the overall regulatory landscape under the PRC law is still in a state of flux. Multiple implementing regulations of CSL are in the pipeline. To name a few, regulations on cross-border transfer, critical information infrastructure, and so on, are expected to further shape the regime. In addition, Personal Protection Law is on the legislative agenda, and businesses in China should closely monitor if the statutory provisions would create a more comprehensive set of rights for the data subject.