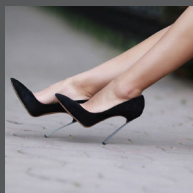
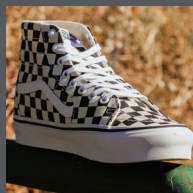


INSIDE



P2 IP LAW

CASADEI:
chi la dura la vince!



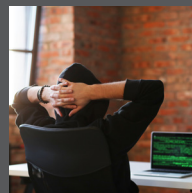
P3 IP LAW

Trademark Infringement:
Don't imitate
Vans Sidestripe



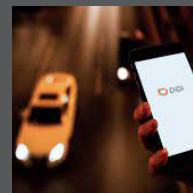
P5 IP LAW

Savio Thesan
succeeds in
patent infringement
in Shanghai



P6 TECH LAW

China's Big Data Era.
New law for
Data Protection



P8 TECH LAW

Didi: the first
cybersecurity review
in China

Dear readers,

Looks like here in China the rain is giving us a break!

Let's treat us with a couple of fashion cases and technology topics.

First of all, compliments to HFG for winning the Casadei case: the final decision from the highest judicial authority – the Chinese Supreme People's Court – posed the word end to the almost-20-years-long legal dispute of the trademark CASADEI for the product of shoes in China.

The second article refers to the trademark infringement of the so-called Sidestripe trademark, which runs along the side of the Vans sneakers. Vans is a quite popular brand in the skateboard world, and that stripe is easy to copy.

Read the article also to get some tips on how the right holder can obtain punitive damages in litigation.

Another case managed by HFG that led to a success is explained in the third article: The Shanghai Intellectual Property Court recognized the patent infringement and awarded damages compensation to Savio Thesan Shanghai.

Talking about technology, we analyze the new, very first law on data security in China. This law provides the legal basis for data supervision, tries to fill the blank of data security protection legislation, and tries to improve the legal system of cyberspace security governance.

Last but not least, the removal of Didi apps from all the app stores, because... read to know why, and to get some takeaways for companies that need to collect and store data.

Additionally, we have something to celebrate this month. Fabio Giacobello and Marco Vinciguerra, HFG Partners, have been re-appointed as the arbitrators/mediators of Shanghai International Arbitration Center's new panel.

Enjoy the sun, stay informed,
read GossIP!

HFG Law&Intellectual Property

HFG

LAW &
INTELLECTUAL
PROPERTY




IP Law


CASADEI: chi la dura la vince!





The Italian sentence “*chi la dura la vince*” means that perseverance overtime brings to success. We quote this sentence in the opening of the article because perseverance was the key to win the present case.

The final decision from the highest judicial authority – the Chinese Supreme People’s Court – posed the word end to the legal dispute of the trademark CASADEI for the product of shoes in China.

 CASADEI trademark was filed for registration in China in May 19, 1999 by an individual person called Zhao Shu Liang for the product of shoes and clothing. After examination the Chinese trademark office granted it for registration with the No. 1453353.

 Once aware of the situation, Calzaturificio Casadei Spa in December 2002 initiated an action to invalidate the trademark on the ground of alleged bad faith of the applicant. The action was rejected in by CNIPA for the lack of sufficient evidence to prove the bad intention of the applicant.

 While the action was still pending, in November 2004, Mr. Zhao filed the trademark again and obtained a new registration with the No. 4342026 from December 2008.

 Later on, in June 2016 the Italian Casadei, still confident in the legal system, filed with the Chinese trademark office an application for cancellation due to 3 years consecutive non-use against both the applications in class 25.

Considering that in facts the trademark was not in actual and sufficient use, this time the non-use cancellation was partially accepted by the Trademark Office.

Unfortunately, the cancellation did not relate the most important product –shoes- for which the applicant filed some evidence of use. Casadei appealed the decision in front of the Beijing IP Court challenging the evidence of use.

In front of the first instance Court Casadei obtained a full success in February 2019, all the goods designated in the trademark were cancelled. The Court found the evidence filed by the trademark owner not enough to uphold the registration.

Nevertheless, the trademark applicant -Mr. Zhao- filed appeal with the higher authority, the Beijing High People’s Court, trying to reverse the first instance decision and to maintain its trademark valid.

CASADEI defended in the appeal phase reinstating that the evidence filed were not proving a sufficient level of use of the trademark. Casadei succeeded again, the trademark was confirmed totally invalid with decision issued in October of 2019.

In 2019 Mr. Zhang filed for retrial of the case in front the Supreme People’s Court in China trying to have the decision repealed also adding some new evidence of use. At last, the SPC issued the final decision on the non-use cancellation of the trademarks No. 1453353 and No. 4342026.

It is worth mentioning that during the non-use cancellation procedure the parties tried to negotiate a transfer of the trademark, however an agreement was never found since the amount of money requested as price of the transfer was very high.

The actions against the trademarks No. 4342026 and No. 1453353 in class 25 were formally initiated in the name of cover entity.

HFG IP and Bugnion Spa have jointly represented the fashion company in the legal battle.


Fabio Giacobello
HFG Law&Intellectual Property


IP Law


Trademark Infringement: Don't imitate Vans Sidestripe



California brand Vans is the label that springs to mind when you think of skate shoes. Vans' two most recognizable design elements are the "Off the Wall" logo - usually located on the tongue or heel tab of its shoes, with its text set within an old-school skateboard - and the Sidestripe trademark, which runs along the side of the sneakers. The Sidestripe, sometimes referred to as the "jazz stripe", appeared for the first time in 1967.





Recently in China, Vans succeeded in a litigation case which confirmed the trademark infringement against Vans' registered trademark for Sidestripe, namely No.8606383 " ".





Plaintiff	VANS, INC. ("Vans")
Defendant	Zhejiang Kaibang Footwear Company Limited ("Kaibang")
Cause of Action	Trademark Infringement
Case Number	(2020) Zhe 0381 Min Chu No. 11073
Court	Zhejiang Rui'an Intermediate People's Court
Decision	1. The Defendant immediately stop the infringement against the Plaintiff's trademark No. 8606383 "  " 2. The Defendant compensate the Plaintiff for economic losses totaling 1,000,000 RMB (including reasonable expenses)

Vans claimed the trademark protection for No. 8606383 "  " in class 25 covering shoes and other goods since September 14, 2011. As a distinct mark of the Vans brand, it has enjoyed high reputation and economic value through long-term use and promotion.

The Defendant was established on September 22, 1999, and its business scope include manufacturing and sales of shoes.

On September 6, 2017, the Ruian City Market Supervision Administration Bureau ("Ruian MSA") inspected the defendant's business premises and found 1950 pairs of shoes bearing the same logo with Plaintiff's trademark on the spot.

Again, on September 16, 2019, Ruian MSA seized 930 pairs of shoes with the "  " logo produced by the Defendant. Later on October 23, 2020, Ruian MSA found 540 pairs of shoes with the "  " and "  " logos produced by the defendant and 1200 uppers with the "  " logo again.

The Court deemed the alleged infringing product prominently used the "  ", "  ", "  " and other logos on the shoe surface, which is a trademark use behavior. Such logos constitute similar mark to Plaintiff's trademark No.8606383 "  " and sufficiently confusing.

The use of similar trademarks on producing and selling the alleged infringing products constitutes the trademark infringement against Plaintiff's trademark right, and should bear civil liability for stopping the infringement and compensating for losses.

Regarding the amount of compensation, since the Plaintiff failed to prove the losses suffered by the infringement, the benefits the Defendant received due to the infringement, and the amount of trademark license fees, thus the statutory compensation should be applied to this case.

When determining the amount of compensation, the multiple and serious circumstances of the infringement shall be fully considered. After being punished in an administrative penalty for infringement, the Defendant continues to commit the same or similar infringement again.

The subjective maliciousness is obvious and the circumstance is serious, thus the punitive damages should be applied.

Therefore, the court finally determined that the defendant should compensate the plaintiff's economic losses totaling RMB 1,000,000 (including reasonable expenses).

Comments on Vans case

Vans' trademark protection for its iconic distinctive element provides more legal bases when defending the rights against the counterfeiters or/and infringers. This reminds the rights holders not to ignore the iconic elements on the product.

Continue reading

According to the Judicial Interpretation, the trial on punitive damages mainly follows the following sequence for the time being:

Determining the established of infringement → Judging subjective intention* → Judging the seriousness of the circumstances* → Determining the compensation base → Determining the multiple of compensation (1 to 5).

Note: Undoubtedly, subjective intention and serious circumstances are the main factors to determine the punitive damages. In practice, it is inevitable that there are overlaps between "*intention*" and "*serious circumstances*", which need to clarify in the future jurisprudence and cases.

Key elements from practice perspective

With the issuance of law including punitive damages and corresponding judicial interpretation, more and more cases start applying punitive damages. In the context of strict protection of intellectual property rights, it is worth thinking about how to obtain punitive damages in litigation for the right holder.

What you can do includes but is not limited to the following actions:

1. Sending C&D letter to the infringer before the lawsuit

If the infringer still does not stop the infringement after receiving the letter from the right holder, it may be preliminarily determined to be "*intentional*".

2. Applying administrative complaints actively

According to the Judicial Interpretation, if the same or similar behavior is executed again after administrative punishment, it can be determined that the "*circumstance is serious*".



3. Enriching the types of infringement evidence

In some cases, if the infringer commits the infringement by means of unfair competition, it can be regarded as serious circumstance. For example, the use of the registered trademarks as domain names, corporate name, and similar decorations to conduct false publicity.

Therefore, if it is found that the behaviors of infringer may constitute unfair competition, the right owner shall fix such evidence together and actively claim in the litigation.

4. Actively initiating criminal-related civil litigation

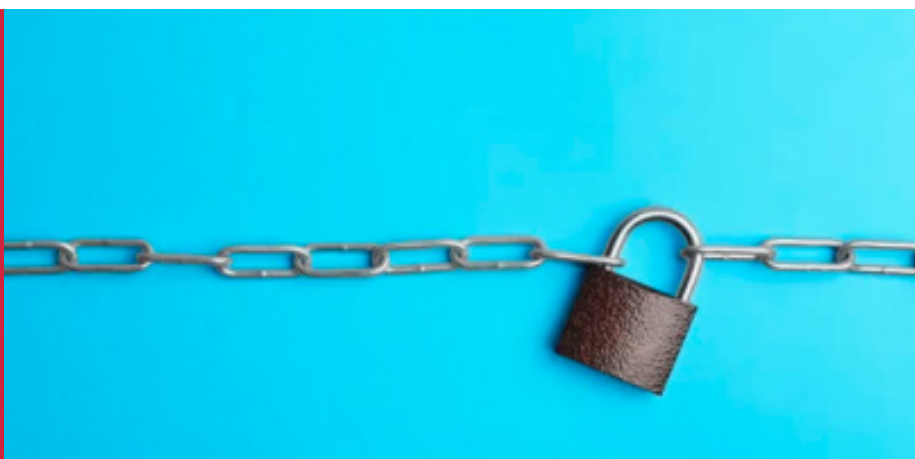
According to the Judicial Interpretation, the defendant committed acts of piracy and counterfeiting of registered trademarks is "*intentions*". In some cases, reaching the criminal standard may directly meet the "*serious circumstances*".

Therefore, the possibility of obtaining huge compensation judgments in criminal-related civil lawsuits has greatly increased, which encourage the right owner to initiating criminal-related civil litigation actively.

Ariel Huang
HFG Law&Intellectual Property

IP Law

Savio Thesan succeeds in patent infringement in Shanghai



With decision issued in June 2021 the Shanghai Intellectual Property Court recognized the patent infringement and awarded damages compensation to Savio Thesan Building Materials Trading (Shanghai) Co., Ltd., a subsidiary of Savio Thesan S.p.A.

The decision is the first of a series of cases initiated by the company to protect its IPRs against copiers assisted by HFG Law Firm in China.

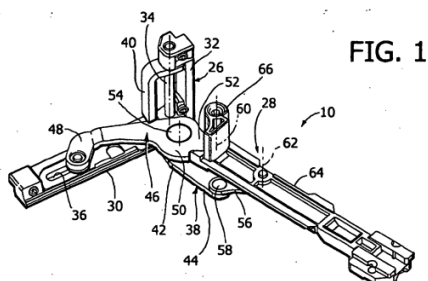
Founded in 1889, Savio Thesan S.p.A. (herein “Savio Thesan”) is a European company leader in hardware for aluminum windows and doors. Headquartered in Turin (Italy), the company has commercial presence in Shanghai, China and other countries.

Savio Thesan has always paid much attention to quality and innovation. Its R&D department employs 51 expert technicians on a total staff of 450 employees (more than 10%!). Savio Thesan has also obtained more than 190 patents in several countries around the world.



Luigi Savio product catalogue (1936)

The Chinese patent ZL 200510081135.6 disputed in the present case at issue is protecting a disappearing hinging device for windows and doors. Herein the drawing No. 1 from the disputed patent.



Talking with Sandro Doveri, GM of Savio Thesan Shanghai, we have learnt that the product protected by the said patent is copied in China by several companies.

“We have decided to put a stop to the infringement to our technology and to initiate patent infringement cases to pursue the infringers” said the manager Mr. Doveri.

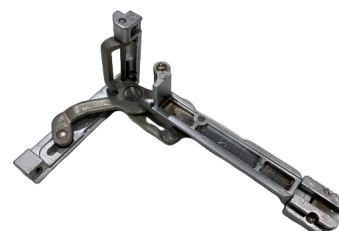


Photo of the product from the Defendant

The Court decisions established that the two defendants shall stop the infringement immediately, shall compensate Savio Thesan the economic loss and the reasonable expenses for rights protection [Shanghai Intellectual Property Court (2020) Hu 73 Zhi Min Chu No. 626 / (2020) 沪 73 知民初 326 号].

The case demonstrates that damages compensation arising from patent infringement and IPRs infringement in general are growing nowadays in China.

This decision shall serve as stimulus to all companies to innovate more, invest more in IP and pursue cases in front of People Courts.

Fabio Giacobello
HFG Law&Intellectual Property

Tech Law

China's Big Data Era. New law for Data Protection



In the past few years, China has digitalized its society at an astonishing pace, and data seem to have become the core asset of the government and companies. As such, national security have risen in China over its data protection, and as a result China's first Data Security Law will go into force soon. It provides for tremendous changes including for Chinese data processors, Chinese data stored outside of China, Chinese data that is required by Foreign governments and heavy fines.

✓ The new law

The Data Security Law ("Law") was officially issued on June 10, 2021 and will be implemented on September 1 of this year.

This Law, together with the Cyber Security Law implemented on June 1, 2017 and the Personal Information Protection Law, forms a comprehensive legal framework in the field of data security, that will protect data and tries to solve data leakage.

Data protection in China under the new regime:



Laws

- Data Security Law
- Cyber Security Law
- Personal Information Protection Law (under the legislation)



Administrative Regulations

- Measures for Data Security Management (draft for comments)
- Measures for Cross-boarder Safety Assessment of Personal Information and Import Data (draft for comments)



National Standards

- Personal Information Security Specification
- Guide for De-identifying Personal Information
- Guide for Personal Information Security Impact Assessment
- Guide for Big Data Security Management
- Guide for Data Cross-board Security Assessment

As the very first law on data security in China, this Law provides the legal basis for data supervision, tries to fill the blank of data security protection legislation, and tries to improve the legal system of cyberspace security governance.

The Law promotes the overall decision-making and coordination of data security to the central national security leading organ for the first time, which is consistent with the National Security Law.

According to the Law, the national security organs, public security organs, national cyberspace administration authority and the competent departments of industry, telecommunications, education, science and technology shall all regulate the data security.

As there are so many state departments involved, it can be seen that data security management goes deep into normal life.



Which data?

Data in this Law refers to any record of information in electronic or other form. It means all kinds of "records of information" kept in any devices like computers, mobile phones, servers and clouds, etc., and the Law puts forward the classified and graded data protection system ("System") to distinguish whether the "records of information" is core data.

In this regard, the Law points out that such System should be established based on the importance of data in the economic and social development, as well as the extent of harm caused by tampering, destruction or illegal disclosure of data.

Continue reading

It is worth mentioning that the Law also emphasizes for the data that have bearing on national security, the lifelines of national economy, people's material livelihood and major public interests shall constitute the core data of the State and shall be subject to stricter management system.

✔ **Duties on data processors**

Data processors will have to set up a data security management system. They will need to appoint a person for data security and have a department for this monitor risks and conduct risks assessments periodically.

In the case of a breach, they will need to take immediate action. For important data they need to work together with the government.

✔ **Data inside and outside of China**

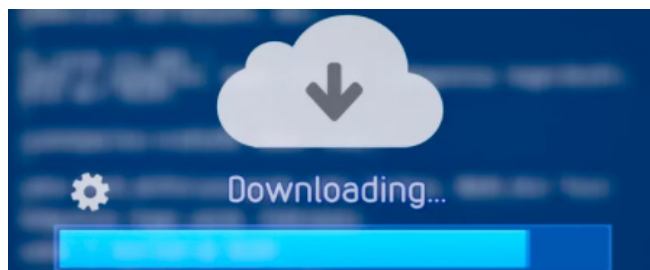
Some companies store Chinese collected data on foreign servers, and the data processing (collection, storage, use, processing, transmission, etc.) involved are also in foreign countries.

The Law stipulates that if the data processing outside of China are found to damage the national security, public interests or the legitimate rights and interests of citizens and organizations of China, they will still be investigated for legal responsibility according to law.

This means that even if the data collected in China is stored on foreign servers, if it involves damaging the legitimate rights and interests, national security of China and other entities in China, the data processor may still face the risk of being investigated for the legal responsibility.

✔ **Need for approval in case of foreign data requests**

Furthermore, without the approval of the competent authorities of China, organizations and individuals within the territory of China shall not provide data stored in the territory of China to foreign judicial or law enforcement organs.



This indicates that if the enterprises are facing the data providing requirements from foreign judicial or law enforcement organs in the future, the provision of domestic data must be approved by the regulatory authorities.

✔ **Heavy fines**

If the data processor violates the national core data management system and endangers national sovereignty, security and development interests, the data processors will face the risk of imposing a fine of more than 2 million RMB but less than 10 million RMB, suspending business, revoking business license, or even pursuing criminal responsibility.

This is also a warning to all data processors that they should always strictly abide by the Data Security Law and relevant rules while enjoying the convenience and economic benefits brought by data, otherwise they will be in a situation where the loss outweighs the gain.

✔ **Companies need to know how to protect whose data where**

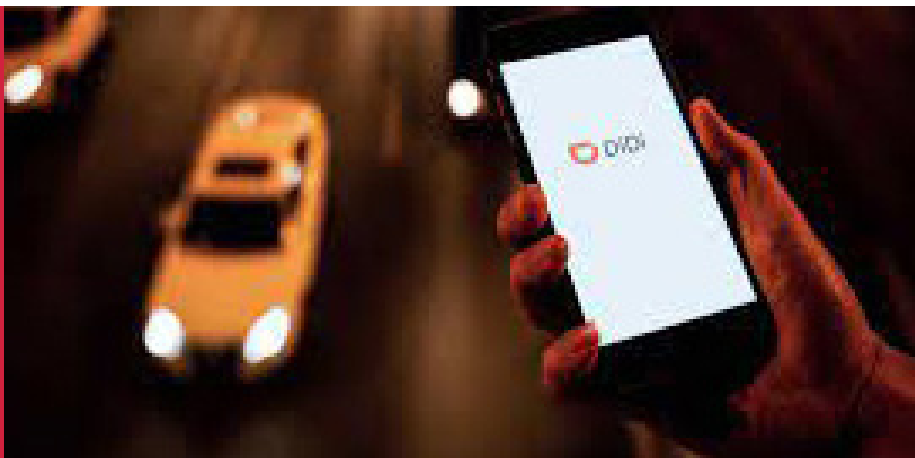
Data is key for China. As such Data protection and national security have become more and more intertwined. For companies it is key to know how data needs to be protected in accordance with China's laws. At the same time, it needs to be checked that this is also in compliance with the laws of other countries.

As such, knowing whose data need to protect in which manner where, will become key in order not to face scrutiny by the Chinese government.

Karen Wang
Reinout van Malenstein
HFG Law&Intellectual Property

Tech Law

Didi: the first cybersecurity review in China



Didi is China's biggest ride-hailing app. At the end of June this year, it was officially listed on the New York Stock Exchange and its market value reached 67 billion USD at the issue price. Just a few days after listing, Didi faced one of the biggest crises in its history. All of its 25 apps were taken offline and its share price dropped.

What happened

On July 2, the Cybersecurity Review Office announced a cybersecurity review on Didi and on July 4, just two days later, it ordered Didi to remove Didi Apps from all App stores. On July 16, the Cyberspace Administration of China, under which the cybersecurity review office operates, together with six other departments jointly launched a cybersecurity review against Didi.

Such a large-scale joint department review is very rare in China. This is the first time that China launched a cybersecurity review on an enterprise. As such, special attention should be paid to how this review will operate in practice.

Illegal collection and use of personal information

The Cybersecurity Law and the Measures for Cybersecurity review provides for a cybersecurity review in order to prevent national data security risks and safeguard national security and public interests. According to the governmental notice, the Didi App has serious problems in collecting and using personal information illegally.

As a leading company in the field of transportation, the Didi App has more than 1 billion users. With such a high number of users, Didi is able to collect a large number of user's personal travel information and high-precision map information. It can be considered that the leakage of this critical information will have a great impact.

Although the final result has not come out yet, we can still learn some experience from it. Several regulations are related in this action, such as the Cybersecurity Law, the Data Security Law, the Measures for Cybersecurity Review and so on.

Which direction is the Cybersecurity Review heading?

On 10 July, a revision draft of the Cybersecurity Review Measures was published for comments. Article 6 mentions that in order to apply for a listing overseas, an operator must apply to the cybersecurity review office for a cybersecurity review if it is in possession of the personal information of more than 1 million users.

The fact that these draft Measures are published so shortly after the Didi listing and cybersecurity review shows that in the future, overseas listings will be more scrutinized for Chinese companies.

In other words, the Chinese government takes a cautious attitude towards data leaving the country. The draft Measures are introduced in order to avoid the leakage of sensitive information and data. In the big data era, critical information has been raised to the level of national security.

The revised Measures also stipulate the factors which will be taken into consideration when assessing the national security risks during the cybersecurity review.

These factors include the security, openness, transparency, diversity of sources, reliability of any supply channel of any product or service and the risk of its supply being interrupted due to political, diplomatic, trade or other factors; the risk of theft, leakage, corruption or illegal use or export of any critical or key data or a large amount of personal information; the risk of any critical information infrastructure, key or important data, or a large amount of personal information being affected, controlled, or maliciously exploited by a foreign government after the company is listed overseas, and other risks.

Continue reading

Take-aways for now: protect data!

We will await the outcome of the cybersecurity review on Didi, and will then see what in practice happens to companies that might not act in accordance with the current laws and regulations in China.

In this regard it is also important to notice that China will have a new Data Security Law from 1 September 2021.

In the meantime, enterprises should pay more attention to data security compliance. For those companies with a small number of users, excessive demand for user's information is likely to increase the cost for operators to protect these data and get into unnecessary troubles.

The more data you have, the greater risk you face. Also, the requirements for the security, openness, transparency and diversity of the products and services supply will be higher.

For larger companies, especially those who are planning overseas listings, they will need to be prepared to face the cybersecurity review and provide solid evidence and demonstration in advance for the data security risks that may be questioned in the review.



Finally, bear in mind that a cybersecurity review might strongly adversely impact on your business. For Didi, many users choose other apps during the cybersecurity review, some users even cancelled their account in Didi because they think their personal information has been stolen.

As such, being on top of data protection in China, seems to be the new reality for companies in China.

Peggy Tong
HFG Law&Intellectual Property

HFG News

HFG Partners appointed as arbitrators of SHIAC



For the third time, HFG Senior Partner Fabio Giacobello has been appointed to be the arbitrator/mediator of SHIAC's new panel from Aug 1st, 2021 to April 30th, 2026.

After Fabio Giacobello, another HFG Partner, Marco Vinciguerra has been re-appointed as arbitrator of SHIAC's new panel until April 30th, 2026.

Established in 1988, the Shanghai International Economic and Trade Arbitration Commission (also Shanghai International Arbitration Center, commonly referred to as the SHIAC) has been providing independent, impartial, effective and professional arbitration services for the commercial dispute all along.

The SHIAC's panel of arbitrators is constituted by arbitrators from 74 countries and regions.

With 30 years of development, the types of disputes include trade, investment, transfer of technology, M&A, finance, securities, insurance, real estate, construction, logistics, intellectual property, franchising, energy, environment interest, information technology.

CONGRATULATIONS!