DLA PIPER

ASIA PACIFIC

INTELLECTUAL PROPERTY AND TECHNOLOGY NEWS

Perspectives • Analysis • Visionary Ideas

JUNE 2017

www.dlapiper.com

IN THIS ISSUE…

EDITOR'S COLUMN

Welcome to the latest Asia Pacific Edition of the Intellectual Property and Technology News, our biannual publication designed to report on worldwide developments in intellectual property and technology law, offering perspective, analysis and visionary ideas.

We're half way through 2017, and it's been an eventful 6 months, as illustrated by this bumper issues of IPT News. In this issue, we've taken a look at the rise of "smart" buildings (page 7); website blocking and piracy in the music and entertainment industries (page 14); and highlighted increasing cyber security risks associated with internet connected devices (page 9).

In China we've delved into the new Cybersecurity Laws which came into effect on 1 June (page 4); and we've provided an interpretation of the Provisions introduced to address substantive and procedural issues in administrative trademark appeals (page 11).

This edition also covers a range of topical IP issues, including how businesses can combat counterfeits (page 16); issues associated with generic marks and names (page 17); and we've provided some insights into the impact of Brexit on trademarks and design (page 18).

We hope you enjoy this issue of the IPT News and that you will take away something new and helpful from it. Please feel free to provide us with any suggestions or feedback that you may have so we can continue to make this publication one you look forward to reading.

Kind regards

Tim Lyons
Head of Intellectual Property and Technology – Australia
tim.lyons@dlapiper.com

Edward Chatterton
Head of Intellectual Property and Technology – Hong Kong
edward.chatterton@dlapiper.com

Horace Lam
Head of Intellectual Property and Technology – China
horace.lam@dlapiper.com

The award – winning *Intellectual Property and Technology News* is now published in the United States, Asia Pacific and EMEA regions. Find all current and past editions of the *IPT News* here: www.dlapiper.com/ipt_news/.

MEET SINEAD LYNCH

Sinead Lynch
Special Foreign Legal Counsel
(Admitted in England and Wales & ROI)
Sydney
T +61 2 9286 8296
sinead.lynch@dlapiper.com

We are delighted to have Sinead Lynch join the IPT team as a Special Foreign Legal Counsel (Admitted in England and Wales & ROI). Prior to joining the DLA Piper team, Sinead worked for over five years as a senior TMT lawyer.

Sinead has significant experience in large scale, innovative sourcing transactions, managed services initiatives, telecommunications procurement and other strategic and complex IT, telecommunications and commercial projects for customers and suppliers in both the public and private sector. Sinead has particular experience advising in regulated industry sectors, including telecommunications, energy and utilities.

How long have you worked at DLA Piper and what brought you to this position?

I joined the Sydney IPT team of DLA Piper Australia as a Special Foreign Legal Counsel in March, 2017.

Having worked on large, complex, innovative and cross border technology transactions, most recently at CMS in London and before that in Dublin, I have always been passionate about technological and cultural innovation. DLA Piper shares my passion: both in the innovative work that DLA Piper does and the firm's global approach to innovation and fostering change. I am also passionate about improving diversity in the workplace, particularly for women and I was really impressed by the Diversity & Inclusion programmes here.

What do you love most about DLA Piper and your job?

The firm's focus on innovation and growth while maintaining client care and firm culture is both forward thinking and refreshing! Working with Mel, Peter, Tim and the wider IPT/Tech sector teams, I have found the clients, prestige and geographical reach expected of a major global law firm with a positive culture, flexibility, care and support for individual team members.

As a technology advisor, my practice supports the full range of ICT – from advising innovative, emerging tech start-ups to supporting large-scale ITOs, BPOs and managed service transactions for FTSE100 global organisations. This also includes specialised advice on privacy and cyber-security related issues. The ability to be able to support the full spectrum on cutting-edge technology projects – across an ever-expanding global network – is fantastic.

The people culture at DLA Piper Sydney is also first class! I am working with great, smart, like-minded people who devote their time and energy into ensuring our clients come first, but who always turn up for a laugh at end-of-week drinks!

If you had Malcolm Turnbull's job for one day, what would you do?

Good question! I found it curious that there has been a shift in focus from technology and innovation in the recent Federal budget. If I was PM for one day, I would reinvigorate incentivisations in the technology and innovation sector, look to refine some of the more recent changes introduced which curb the technology sector (such as the proposed changes to the 457 visa system), and before nightfall, I probably would not be able to resist the urge to lift the phone to Donald Trump for a bit of a side bar on life generally!

If you could invite three people for dinner, dead or alive and excluding family and friends, who would they be and why?

That's easy! Steve Jobs, because there are just so many questions to ask; Michelle Obama, simply inspirational and Brian O'Driscoll, the world's best rugby player!

PRC CYBERSECURITY LAW

Take action and monitor developments to avoid losing your China business

BY SCOTT THIEL, CAROLYN BIGG & PAULA CAO (HONG KONG)

The PRC Cybersecurity Law is three weeks old, and non-compliant international businesses are already facing severe consequences. Since 1 June, twenty-two people engaged by a global technology giant have been arrested, and sixty online entertainment news sites have been shut down.

The law continues to evolve. The latest guidance provides practical answers to previous areas of uncertainty. Whilst some questions remain, the key message is: do not ignore the PRC Cybersecurity Law. It is now in force and organisations must comply with it.

Read on if you:

- Transfer personal information and important data out of China
- Are concerned your organisation may be a key information infrastructure operator
- Supply network and cybersecurity products and services to China
- Are unsure if you handle "important data" in or from China

Five key developments that you need to know

1. What is now in force?

- The data protection and data security obligations on network operators and key information infrastructure operators (KIIOs) came into force on 1 June 2017
- The supervisory assessment/certification scheme for suppliers of critical network and specialised cybersecurity products and services also came into force on 1 June 2017

2. Are the new overseas data transfer rules in force?

Not yet. The draft measures proposing conditions/restrictions on overseas transfers of personal data and important data by network operators including KIIOs (Draft Measures) did not come into force on 1 June 2017, surprising commentators. Unofficial sources indicate the lead regulator (CAC) discussed a revised draft of the Draft Measures with key stakeholders and proposed toning down some of the more onerous obligations. For now, we await official announcements from CAC.

If and when the Draft Measures come into force, organisations should follow the newly-published *Draft Guidelines for Data Cross-Border Transfer Security Assessment* (Draft Guidelines). These set out detailed guidance on the security self-assessments for cross-border transfers. They include practical tips on how and when to conduct a self-assessment, including key factors to consider (legality, legitimacy, control of risks, technical and management skills, the recipient's capability to protect data, and the recipient countries' political and legal environment), and a rating system to apply. Practical examples are also given on how to assess the sensitivity and level of influence of personal/important data, and solutions to minimise the risks.

3. Am I a KIIO?

- We still don't have a definitive answer, but previously unofficial guidance has now been formally published. The *National Internet Security Check Operational Guideline* is primarily a guideline for Government agencies. A key infrastructure protection regulation is being prepared by the Chinese authorities (which may or may not refer to this guideline) and (according to CAC) is expected to be published for public comment soon. It is hoped this regulation will provide greater certainty. For now, who does the guideline indicate will be deemed a KIIO?
- Websites: operators of:
  - Party/Government websites
  - Key news websites
  - Websites with more than one million visits per day
  - Websites where a network security incident would have a significant impact (i.e. on work/lives of over one million individuals or 30% of a district; disclosure of personal information of over one million individuals; disclosure of large volumes of sensitive corporate

information or "national basic data" (relating to resources, mapping); or damage to/endanger government image, social order or national security)

- Platforms: operators of platforms:
  - With registered users over ten million, or with over one million active users (with a login frequency of at least once a day)
  - With average daily orders or transactions over RMB 10 million
  - Where a network security incident would have a significant impact (i.e. direct economic loss of RMB 10 million or above; on work/lives of over ten million individuals; disclosure of personal information of over one million individuals; disclosure of large volumes of sensitive corporate information or "national basic data" (see above); or damage to/endanger government image, social order or national security)
- Production Businesses:
  - Operators of systems for public/government/cities such as healthcare, security, fire service, emergency management, production scheduling, traffic control
  - Operators of data centres with over 1,500 standard servers
  - Businesses where a network security incident would have a significant impact (i.e. on work/lives of 30% of a district; affect the utilities or transport of at least 100,000 individuals; death of five or more individuals, or serious injuries to fifty or more individuals; direct economic loss of RMB 50 million or above; disclosure of personal information of over one million individuals; disclosure of large volumes of sensitive corporate information or "national basic data" (see above); or damage to/endanger government image, social order or national security)

4. Can I still sell my technology products in China?

Yes, but you now need to consider the supervisory assessment/certification scheme for suppliers of critical network and cybersecurity products and services to KIIOs or to be used for other networks and information systems that relate to national security. We now have an initial catalogue of those caught by the new scheme:

Critical network equipment	Specialised cybersecurity products
Routers	All-In-One data backup
Switches	Firewall (hardware)
Servers (rack-mounted)	Web application firewall
Programmable logic controllers	Intrusion detection system
	Intrusion defence system
	Security isolation and information exchange products (gatekeeper)
	Anti-spam mail products
	Network integrated audit system
	Network vulnerability scanning product
	Security data system
	Website recovery products (hardware)

The new *Trial Measures for Security Review of Network Products and Services* (Trial Measures) provide practical guidance on how the scheme will be implemented. Whilst uncertainties remain, the Trial Measures clarify that:

- Reviews will focus on "security and controllability" risks of products and key components, from manufacture through to sale, implementation and maintenance/support. Initially TC260 standards have been released for evaluating security and controllability of central processing units, operating systems and office software
- Competition impact is a lesser concern, but reviews will look at dependence on certain providers
- Reviews will also consider risks of providers accessing data and user information through their products/services
- Reviews may be conducted in a lab, onsite, remotely or through background investigations. While some technical documentation must be provided, it is not yet clear whether source code must be disclosed; and what sort of test environment providers may need to make available to the authorities

5. What is "important data"?

"Important data" is broadly defined to include information that relates to national security, economic development, or social or public interest. Appendix A of the Draft Guidelines sets out an 11-page list of examples in key sectors such as utilities, telecommunications, geographical information, finance and e-commerce. The coverage is very broad, and is a useful reminder to organisations that the PRC Cybersecurity Law does not just affect personal data and has a very wide reach.

What other developments are anticipated?

Issue	Development	Impact
General personal data protection	*Draft Information Security Techniques – Personal Information Security Specifications*, published for public consultation and, according to reports, expected to be implemented soon. This is in effect an update to the 2013 general data protection guidelines governing personal data, which is the current persuasive best practice, and practical guidance, on how to handle personal data in China	**High:** first statement of key data protection principles in China; significant changes to key terms such as "sensitive personal data" and "data controller"; greater clarity on clarity of privacy notices and terms to be included; additional security measures; and new DPO requirements
Minors' data	*Draft Regulations on the Protection of the Use of Internet by Minors*, published for public consultation in January 2017	**Medium:** additional protections for minors' online, including safeguards for collection, use and disclosure of minors' personal data by "network information service providers"
Encryption	*Draft PRC Encryption Law*, published for public consultation in April 2017	**High:** more standardised approach to encryption and IT security in China (including mandatory national standards); use of encryption would be mandatory for some networks and data; encryption will remain heavily regulated; requirement for suppliers to provide decryption support
Consumer data	*Draft Regulations on the Implementation of the Law on the Protection of the Rights and Interests of Consumers*, published in Summer 2016	**High:** strengthening of consumer personal data protection, including consent, mandatory data breach notification and record retention requirements
E-commerce data	*Draft E-commerce Law*	**High:** new data protection obligations including prior notice consent; explicit consent for subsequent changes of scope/ purpose; data retention, use and security obligations: immediate data breach notifications: and irretrievable anonymisation of e-commerce data before disclosure

SMART BUILDINGS – NOT JUST BRICKS AND MORTAR

BY SINEAD LYNCH AND CLAIRE KERMOND (SYDNEY)

Imagine a day where any part of a building can report its own state of health, when a machine can tell you if its feeling unwell and 'needs a service', when you can track and prevent, before it happens, a water or gas leakage – all from the convenience of your own smartphone or laptop at home.

This is no longer imagination – this day is now!

The real estate industry is fast becoming influenced by rapid technological advancements. Technology is a significant source of disruption and opportunity particularly in buildings and modern infrastructure. Buildings are changing, they are no longer just bricks and mortar. While it's not new for technology to form part of the inner workings of a building, sophisticated and advanced technologies are now being integrated into underlying designs and building management systems that underpin most modern building structures. These building management systems are no longer fully segregated from conventional IT networks, such as servers, customer relationship management or online payment systems. Buildings are becoming more mobile, flexible and connected – in effect becoming 'smart'.

Landlords, tenants and owners are becoming increasingly reliant upon, and are leveraging, sophisticated new technologies in the day to day use of spaces, resulting in greater amounts of data being captured in buildings, office towers and homes around the country. Digital technology is reportedly being used by owners and landlords to assist in brick and mortar sales. For example – in retail centres, with the goal being to guide a customer from the start of their product acquisition right through to purchase i.e. a customer searches for a product on Google, finds the product at the shopping centre, is digitally guided by the landlord/centre to an open parking space at the property and then to the store to collect the product.

In hotels, cashless payment technologies are used to increase on-site spending patterns. In offices, mobile and wireless technologies support recent trends towards more open and collaborative workspaces. Employee movements around a floor can be recorded – the resulting data can be put to multiple uses – i.e. by staff to work out where may busy or quiet in the office or by organisations to cut cleaning costs, allowing them to focus on cleaning busy areas rather than unused areas. Lighting, humidity and temperature can all be pre-recorded and customised, window coverings can be programmed to block harsh light at certain times of the day, security passes can record movements and time entries, or indeed facial recognition can replace card activation altogether.

It's abundantly clear that such 'smart' buildings are invaluable for landlords in automating building management systems, for employers in improving workplace management and the work environment, and for tenants in increasing footfall to their unit. The data collected can be put to a myriad of uses, including increased efficiency and reduced maintenance costs. But, as with all big data collection, the use, storage and processing of personal information, raises a number of specific privacy, security and contractual issues for all involved.

In particular, employers need to consider the impact of workplace surveillance legislation and regulations

in a number of States and Territories and the Privacy Act 1988 (Cth) when collecting data relating to their employees and ensure that they have appropriate arrangements in place to notify their employees in advance of any potential surveillance.

Landlords, tenants, operators and managers must all be cognisant of their legal obligations and responsibilities in complying with applicable privacy laws when collecting personal data. Are you collecting more than you need or holding for longer than necessary? When a data breach occurs that causes serious harm to an individual, are you aware of your obligations under the new mandatory data breach notification requirements?

If this breach impacts more than one individual (i.e. tenants of a building), who is liable? How has contractual liability for personal data breaches been apportioned? Do you know what action to take if the building becomes a target for cyber criminals? How current are your incident response plans? When were they last tested?

Security breaches in smart buildings are becoming increasingly common with cyber criminals targeting vulnerable building management systems, for example the most recently reported attack on government facilities. Retailers and tech giants are also not immune with Google's building management system in Sydney being infiltrated by researchers seeking to prove a point. It goes without saying that apart from the costs, the significance of data and security breaches can cause (sometimes irreparable) damage to an organisation's reputation and bottom line. The recent vulnerability in Target's HVAC platform allowing access to the credit card information of millions of customers being a case in point.

The most recent ransomware cyber-attack 'WannaCry' which impacted multiple organisations and governments in over 150 countries around the world, brings home to all of us the inherent vulnerability in many organisation's existing infrastructure to cyber-attacks. Albeit outdated software was the focus in this incident, the importance of security vigilance by all organisations cannot be overstated. In Australia, smaller businesses in particular are also at greater risk, according to a recent cyber report from the Turnbull government.

Owners, landlords and tenants of smart buildings would be wise to closely consider their data and security protocols and the types of information and data they may be collecting through the use of advanced systems in buildings and how best to protect users from exposure of personal information. Cybersecurity and data protection are not just issues for the IT department, they are business critical issues which must be addressed at the highest level. Advanced data encryption, tested security protocols, privacy and security by design processes, compliant data policies and procedures and a heightened awareness of these issues and risks will ensure a long reign to the smart buildings of our future.

IoT GOT 99 PROBLEMS AND SECURITY IS ONE

BY NICHOLAS BOYLE AND CLAIRE KERMOND (SYDNEY)

The number of internet connected devices and products is rapidly increasing and in turn creating more opportunity for cyber security breaches and generating greater amounts of data including personal information. Consumer fear is also heightened around this issue – the recent Australian Community Attitudes to Privacy Survey 2017 revealed that 83% of Australians perceive the online environment to be more risky and only 10% of Australians are comfortable with their personal data being shared.

Cyber criminals and hackers have targeted some 'internet of things' products, perhaps because of the perception (which in some instances has been reality) that manufacturers of traditionally 'unconnected' devices (e.g., kettles, toys, dog bowls, vacuum cleaners) have been less attuned to the security challenges associated with internet connected devices. There also appears to be a public perception in some instances that the data collected by many IoT devices is less 'valuable' to criminals than, for example, financial information collected and held by banks, retailers and others, and therefore is a less likely target of attacks.

But that sort of thinking overlooks other potential risks associated with the way in which IoT devices may operate and the different ways such devices could be compromised or exploited by criminals or hackers. For example, concerns were raised with two internet connected toys – the 'My Friend Cayla' doll and 'i-Que Intelligent Robot' – which engaged in conversations with children. These toys recorded conversations and could be hacked, allowing hackers to listen back to the recorded conversations and control what the toy said in response to questions. The privacy concerns with the dolls resulted in the 'My Friend Cayla' doll being banned in Germany.

On a larger scale, IoT devices can be attacked by malware to compromise networks and turn devices into botnets (i.e., groups of devices that are centrally controlled). Cyber criminals successfully used the Mirai malware in October 2016 to hack IoT devices and flood websites with traffic to launch a distributed denial of service attack against popular domain name service provider Dyn which resulted in the outage of websites such as Twitter, the Guardian and CNN. IoT is only just beginning, and the security risks that come with it will become more complex as it grows. The proliferation of IoT devices – expected to be more than 20 billion internet connected devices by 2020 – means that there potentially is a very, very large number of devices that could become botnets used to disrupt other websites.

Taking all these factors into account, information security should be a key focus for organisations involved in any part of the IoT ecosystem – whether it be manufacture, implementation and integration or retail. Steps that organisations can take to mitigate the risks of data breaches or incidents, and the impact arising from such a data breach or incident, include the following:

- Adopting a 'security by design' approach when designing, developing and implementing IoT devices
- Maintaining and regularly updating appropriate IT security policies and procedures, personnel policies, and device level policies
- The development and implementation of effective compliance training and personnel education processes to foster an environment in which the crucial importance of effective data management and security is understood
- Designing and implementing an internal feedback loop to monitor and identify possible and actual security risks and issues, and ensuring that the impact of major changes is addressed in relevant policies and processes
- Management and governance policies and processes implemented in relation to external vendors including gateway reviews to monitor compliance with mandatory security requirements and other contractual obligations
- Developing and implementing an incident response plan for specific data breach or security issues, and a process for periodic review and updating of the plan. Such incident response procedures must be regularly tested, and changed where necessary. A post incident review should also be performed and documented following any significant security incidents

Data breaches and incidents arising in connection with IoT devices may also be subject to the data breach notification regime which is due to commence in February 2018. This regime will require entities to report serious data breaches to customers, the Privacy Commissioner and potentially to the media, with significant penalties of up to AUD1.8 million for non-compliance.

Read our blog for more information on the upcoming mandatory data breach reporting legislation.

JUDICIAL INTERPRETATION GOVERNING **ADMINISTRATIVE TRADEMARK APPEALS EFFECTIVE 1 MARCH 2017**

BY HORACE LAM, EDWARD CHATTERTON AND REKING CHEN (CHINA AND HONG KONG)

On 10 January 2017, the Supreme People's Court of China (the SPC) promulgated a judicial interpretation concerning trademarks, entitled *the SPC Provisions on Certain Issues Related to Trials of Administrative Cases Involving Grant and Confirmation of Trademarks* (the Provisions). The drafting of the Provisions started in 2013, when the recent amendments to the Trademark Law (the Trademark Law 2013) were enacted. The Provisions became effective on 1 March 2017.

This judicial interpretation is refined and summarized not only from past advisory guidance (notably an opinion issued by the SPC in 2010 for the same area), but more practically from recent cases and opinions issued by various courts. The Provisions consist of 31 articles covering both substantive and procedural issues in relation to trials of administrative trademark appeals. Below is a brief summary of the key rules introduced in the Provisions.

Scope of Review

Under the Provisions, the court's scope of review for administrative trademark matters are confined to various decisions issued by the Trademark Review and Adjudication Board (the TRAB), including the decisions for reviews on refusal, invalidations, reviews on non-use cancellation, and reviews on invalidation decisions (made by the China Trade Mark Office).

As a general rule, the court should conduct the review based on the **claims of the plaintiff.** However, the Provisions also authorize the court to expand the scope of the review if the court considers the relevant determination of the TRAB evidently inappropriate after hearing the statements of opinion by the parties.

The laws have been ambiguous regarding whether the TRAB's violation of the statutory procedures in deciding cases is subject to judicial review. Whilst it is clear that the TRAB should make decisions in accordance with procedural rules set out under the Trademark Review and Adjudication Rules issued by the State Administration for Industry and Commerce, there have been no statutory provisions on penalties to the TRAB or resorts to the parties in case of the TRAB's violation of the statutory procedures. The Provisions now enumerate circumstances where the court can overrule the TRAB's decisions for 'violated statutory procedures': (1) the arguments for review that actually affects the right of the parties have been omitted; (2) the identity of the panel has not been notified to the parties, such that a member subject to recusal fails to be recused; (3) the appropriate party to the matter has not been duly notified and it raised objections; (4) any other situations that are in violation of the statutory procedures.

Protection of Well-Known Trademark

The Provisions enumerate multiple factors to consider when determining whether there is 'likelihood of confusion' or 'damage to the well-known mark', which is significant for protection of unregistered and registered well-known trademarks respectively.

A. For **unregistered well-known trademarks**, the court shall consider the following factors for determination of confusion:

(1) the extent of similarity of the two trademarks; (2) the extent of similarity of the goods of concern; (3) the distinctiveness and reputation of the alleged well-known mark; (4) the extent of the perception of the relevant public; (5) any other relevant factors. The intent of the trademark applicant and evidence of actual confusion may also be taken into account in determining likelihood of confusion.

B. For **registered well-known trademark**, in determining whether the trademark at concern would cause damage to the interests of the registered well-known trademark holder, factors to consider are: (1) the distinctiveness and reputation of the trademark alleged to be infringed upon; (2) whether the two trademarks are sufficiently similar; (3) the goods designated for use; (4) the overlapping and perceptions of the relevant public; (5) other's legitimate use of trademarks that are similar to the alleged well-known mark.

C. When determining bad faith (which is a key condition to get around the general 5-year time bar against invalidation post registration), the court should take into consideration: 1) the reputation of the alleged well-known mark; 2) the applicant's reasons for the application; and 3) how the applied-for mark is being used. The court may presume the bad faith if the alleged well-known mark is very famous in China and the applicant fails to provide a justifiable reason for the application.

Principle of Good Faith

The Trademark Law 2013 included a new article stressing that the 'principal of good faith' shall be followed in the registration and use of a trademark. The Provisions echoes such legislative intention in many aspects.

A. Article 15(1) of the Trademark Law 2013 prohibits an agent or a representative from applying or using the trademark of the principal or the represented party without authorization. The Provisions interpret the term 'agent or representative' in a broad way to include 1) trademark agents; 2) sales agents; 3) persons under on-going negotiation for an agency or representation relationship; and 4) relatives of the above-said agents or representatives.

B. Article 32 of the Trademark Law 2013 provides a limited scope of protection to unregistered trademarks that have been put into use in China, in that no applicant is allowed to pre-emptively register another's prior used trademarks with certain reputation in unfair means. The Provisions introduces three implementation rules for such mechanism, 1) a presumption of unfair means can be made if the prior used mark has accrued certain reputation, such that the applicant is aware or should be aware of the prior used mark; 2) the senior user should produce evidence to prove prior use of the mark in sales and/or promotional activities for a continuous period of time in a certain area of China; and 3) the protection should be limited to identical and similar goods.

C. There has been a great deal of back and forth on the interpretation of 'other illegitimate means' provided under Article 44(1) of the Trademark Law 2013. In the past few years, the prevailing opinion in the industry has been that Article 44(1) is only applicable to registrations which impair public interests. The Provisions changes the situation by providing that 'other illegitimate means' here should include means used to pursue illegitimate interests, which should not be confined to public interests only.

D. Albeit that there are no explicit statutory provisions on the issue, the trademark authorities have been consistently rejecting hijacking trademark applications against the names of celebrities by invoking a general provision of "unhealthy social influence" under Article 10(1) of the Trademark Law 2013. Such practice is now endorsed by the Provisions.

Prior Rights, especially Merchandising Rights

Article 32 of the Trademark Law (2013) requires that trademark applications shall not infringe upon the existing 'prior rights', but fails to elaborate what kinds of rights can be asserted as 'prior rights' here. The

Provisions provides a further enumeration, which remarkably includes merchandising rights for the first time.

A. Prior copyright

The court shall review according to the Copyright Law and the relevant regulations whether the asserted subject constitutes a work, whether the party is the copyright holder or is interested in the alleged copyright, and whether the trademark in dispute infringes upon the asserted copyright. Evidence such as sketching of the designs of the trademark, contracts showing ownership of the right, and copyright registration certificates are acceptable as prima facie evidence on the copyright ownership, whilst trademark registration certificates and trademark gazettes can be accepted as proof of the petitioner's standing in asserting copyright infringement claims (there is a standing requirement to file oppositions and invalidations under the Trademark Law 2013).

B. Right of personal name

The court shall decide that the right of a personal name is violated if the relevant public contemplate that the trademark of concern refers to that natural person, and are likely to think that the goods bearing the mark are authorized by or related to that natural person.

Special names, such as pseudonym, stage names or ***translations of names*** also constitute prior right if these names have a certain reputation and are used to refer to that natural person by the relevant public.

C. Character/name of the work/name of the role *(Article 22)*

Copyright of the Character. The character of a work can be protected by copyright. Therefore, the court shall review infringement claims of such right pursuant to the Copyright Law and the relevant regulations as introduced above.

Names of the works or names of the roles can also constitute a prior right within the duration of the copyright protection if they are well-known, and use of the trademark at concern are likely to mislead the relevant public to consider that the goods bearing the mark are authorized by or related to that owner. This prior right is apparently introduced to solve the problem caused by the hijacking trademark applications against names of famous works and/or roles/characters within such works (e.g. movie names), which has been under heated discussions in the recent years.

Res judicata

The legal principal of res judicata requires that once a matter has been adjudicated by a competent court in legitimate procedure with final decisions/judgments, it should not be heard again by the court on grounds of the same facts and reasons. The Provisions introduces additional rules to this principle.

A. If there is finding of new facts or new evidence, the principle of res judicata may not be applied.

B. Once a court judgment has become effective and the TRAB makes a new decision as directed by such judgment, such decision is not subject to further administrative appeals.

In February 2016, the Legislative Affairs Office of the State Council of China published the draft Amendment to the Anti-Unfair Competition Law (the 'Revision'), for public consultation. This is the first major revision to the current Anti-Unfair Competition Law (AUCL) since it was enacted 23 years ago.

The highlights of the Revision concern unfair competition acts in relation to trade names and the practical administrative penalties regarding use of improper trade names. As the law currently stands, the AUCL does not provide specific provisions or penalties for using others' registered or unregistered trademarks unfairly in one's trade name, despite both the Trademark Law and the judicial practice referring to such behavior as "unfair competition conduct". The absence of specific provisions in the AUCL has caused considerable difficulties in both administrative and judicial actions.

In addition, under the current AUCL, when a prior IP rights owner successfully obtains an administrative decision or judicial judgment ordering change of an improper trade name, such change can only occur upon the accused operator's request. This has caused major enforcement issues as most accused operators decline to file the name change request. The Revision has proposed changes to the law to help resolve these practical issues.

Article 5 – Unfair competition in connection with trade names

Although it is not clearly stated in the current AUCL, it has been an established rule of judicial practice that it is an unfair competition conduct if an operator benefits from unfairly using other's registered or unregistered trademark in its trade name. To fill in this gap in legislature, Article 5.3 of the Revision articulates that "a business operator cannot use another's registered trademark or unregistered well-known trademark as the trade name in its enterprise name, and thereby misleads the public and causes market confusion".

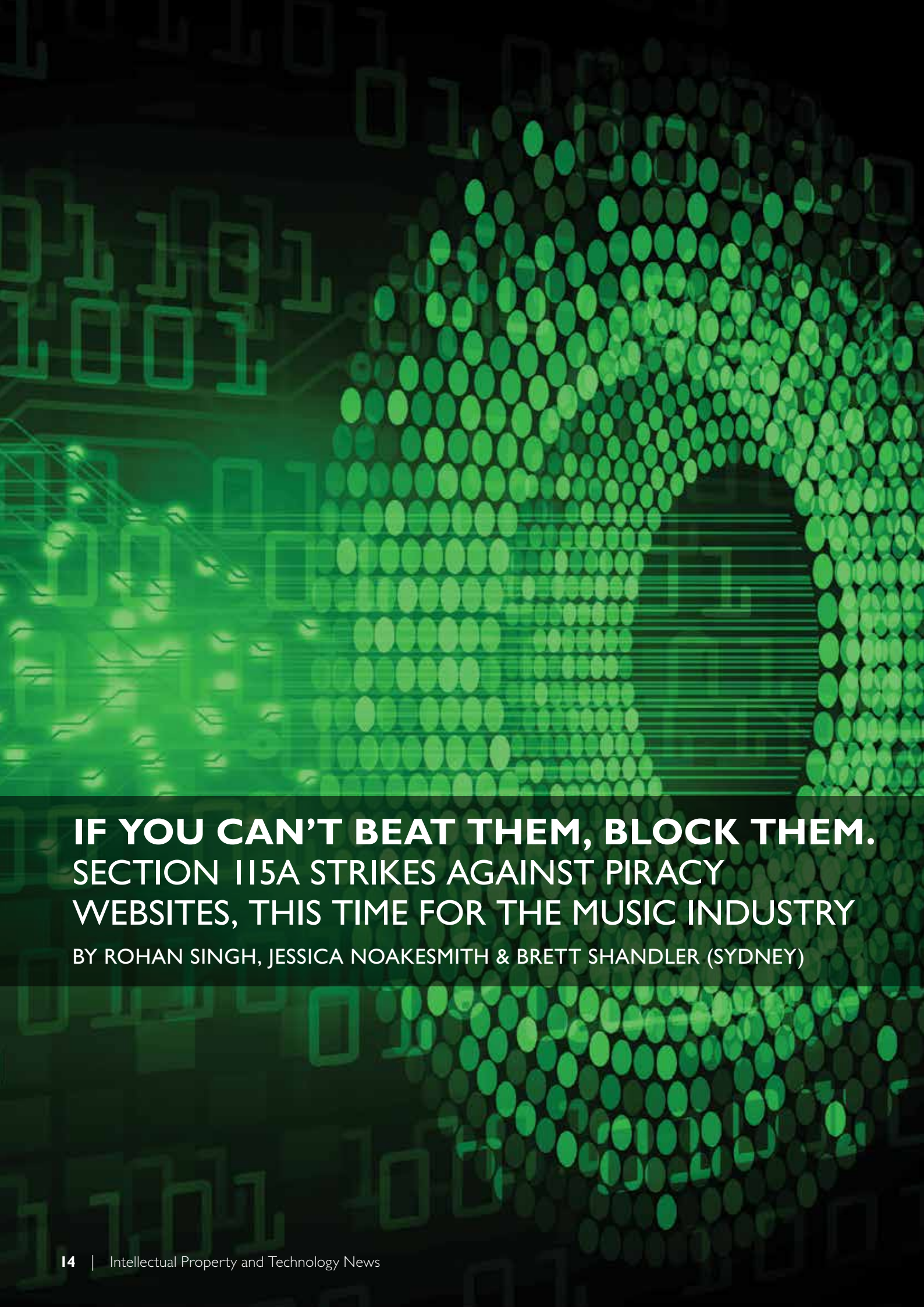
Further, Article 5.4 of the Revision also introduces a new rule prohibiting use of another famous enterprise's trade name or short name as the dominant part of a trademark or domain name. This rule most notably incorporates a test of "market confusion" when determining the unfair competition behavior. This is apparently a higher standard, as compared to the likelihood of confusion standard in finding trademark infringements.

Practical administrative penalties for violation of Article 5.3

The administrative penalties proposed in the Revision appear far more practical than the current practice in relation to one's use of another's registered trademark/ unregistered well-known trademark as a trade name, as provided for in Article 5.3. Specifically, the current AUCL does not provide any practical means to enforce an administrative order or a judicial judgment on a change of an improper trade name when an accused operator fails to comply with these orders. The Revision in Article 18.2 moves a step forward by granting the relevant Administration for Industry and Commerce (AIC) a broad power to remove the enterprise name from the enterprise credit information publication system by replacing it with a registration number or an uniform social credit code as well as putting the enterprise on the List of Enterprises with Abnormal Operations. In severe circumstances, the AICs may also revoke the business operator's business licence.

Notably, Guangdong province has published the Regulations of Guangdong Province on Commercial Registration on December 3, 2015 to reflect such change in practice. The Regulations clearly authorize the AICs in the Guangdong Province to replace any questioned trade name with an uniform social credit code. These Regulations became effective on March 1, 2016.

Public consultation of the Revision closed on March 25 and the State Council will now consider further amendments, before finalizing the Revision for review by the National People's Congress's standing committee.



IF YOU CAN'T BEAT THEM, BLOCK THEM.

SECTION 115A STRIKES AGAINST PIRACY WEBSITES, THIS TIME FOR THE MUSIC INDUSTRY

BY ROHAN SINGH, JESSICA NOAKESMITH & BRETT SHANDLER (SYDNEY)

Universal Music Australia Pty Limited v TPG Internet Pty Ltd [2017] FCA 435 (28 April 2017) (**Universal Music**).

Recently in the Federal Court of Australia, over thirty internet service providers (**ISPs**) including TPG, Optus and Telstra were ordered to block access to the torrenting website KickassTorrents and related domain names. *Universal Music* is the third case to be decided under the recently added section 115A of the *Copyright Act 1968* (Cth) after *Roadshow Films Pty Ltd v Telstra Corporation Ltd* (**Roadshow Films**) and *Foxtel Management Pty Limited v TPG Internet Pty Ltd*[1], and represents a win for music labels such as Universal Music, APRA, AMCOS and Warner Music.

In concluding that it was appropriate to grant an injunction, Justice Burley found it was relevant that Kickass Torrents had been blocked in other countries and that it reflected a flagrant and "open disregard for copyright". Last year the alleged owner of the website was arrested by the U.S. Government in Poland and was charged with criminal copyright infringement.

The ISPs did not oppose the website blocking order, but all (except for Foxtel Broadband) argued that the music labels should cover some or all the costs of compliance as they were innocent parties, and the order ultimately serves to benefit the labels. Justice Burley agreed, and adopted the reasoning in *Roadshow Films* ordering that the ISPs block the nominated websites within 15 business days, for a period of three years and for a nominal fee of $50 per domain name. Relevantly, it was left to the ISPs to cover their own costs in implementing these blocking orders.

To obtain an order under section 115A, a copyright owner must show that[2]:

1. the carriage service provider (ISP) provides access to an online location outside Australia;
2. the primary purpose of the online location is to infringe, or facilitate the infringement of copyright; and
3. the online location infringes or facilitates the infringement of copyright.

For those copyright owners who may be interested in seeking a similar order, this case is informative as to what is necessary to dispense of the requirement for service of the proceedings on the owner of the website, and the evidence that is required to prove that the geographical location is outside of Australia (including using 'ping tests' and 'whois' searches).

This section is proving effective in practice (except for those Australians circumventing the efforts with private VPNs), however time will tell whether the Federal Court will create a separate list or docket to streamline proceedings. The list could potentially provide for standard orders which could incorporate a variation order for additional domain names as was the case here. These websites reproduce quickly and could be better combated through a streamlined list.

The future of website blocking and piracy

ISPs are no longer a passive vehicle for data and this case adds to the responsibilities created by the *Dallas Buyers Club*[3] in identifying names of infringing consumers. All ISPs should set up a system where they can comply with any injunctions under section 115A.

Judgment is still pending for *Roadshow Films Pty Ltd & Ors v Telstra Corporation Limited & Ors*, a subsequent case on section 115A heard 10 May 2017, in which the applicants have sought to have websites Putlocker and Megashare blocked.

If actions under this section prove popular it will be interesting to see if a similar provision is added to the Trade Marks Act 1995. Last year the Court of Appeal of England and Wales upheld an order to block certain websites that infringed or facilitate the infringement of trade marks, as it felt it was appropriate to do so under a general injunctive power[4].

[1] [2016] FCA 1503

[2] *Roadshow Films Pty Ltd v Telstra Corporation Ltd* [2016] FCA 1503 [31]; *Universal Music Australia Pty Limited v TPG Internet Pty Ltd* [2017] FCA 435 (28 April 2017) [14]

[3] *Dallas Buyers Club LLC v iiNet Limited* (No 3) [2015] FCA 422

[4] *Cartier International and Others vs BSkyB and others* [2016] EWCA Civ 658

IS IT THE REAL MCCOY?
ANTI-COUNTERFEITING, IP RIGHTS AND YOUR BUSINESS

BY ROHAN SINGH & JESSICA NOAKESMITH (SYDNEY)

A recent report based on customs' seizures by The Organisation for Economic Co-operation and Development (OECD) found that fake information and communications technology (ICT) goods accounted for 6.5% of the overall ICT trade, well up on the 2.5% of overall traded goods found to be fake in a 2016 report. The report included both final products and intermediary parts such as network components and communications hardware, and concluded that nearly one in five mobile phones and one in four video game consoles shipped internationally is fake. This is not a shock as the steady demand for products in the ICT sector is a lucrative target.

Counterfeits are products that infringe trade mark with the intent of passing them off as authentic. As ICT goods are more complex than say fake handbags, the average consumer cannot tell the difference between a branded smart phone and a counterfeit phone or component. The effect of counterfeiting is widely felt by businesses across in the ICT sector in many regions.

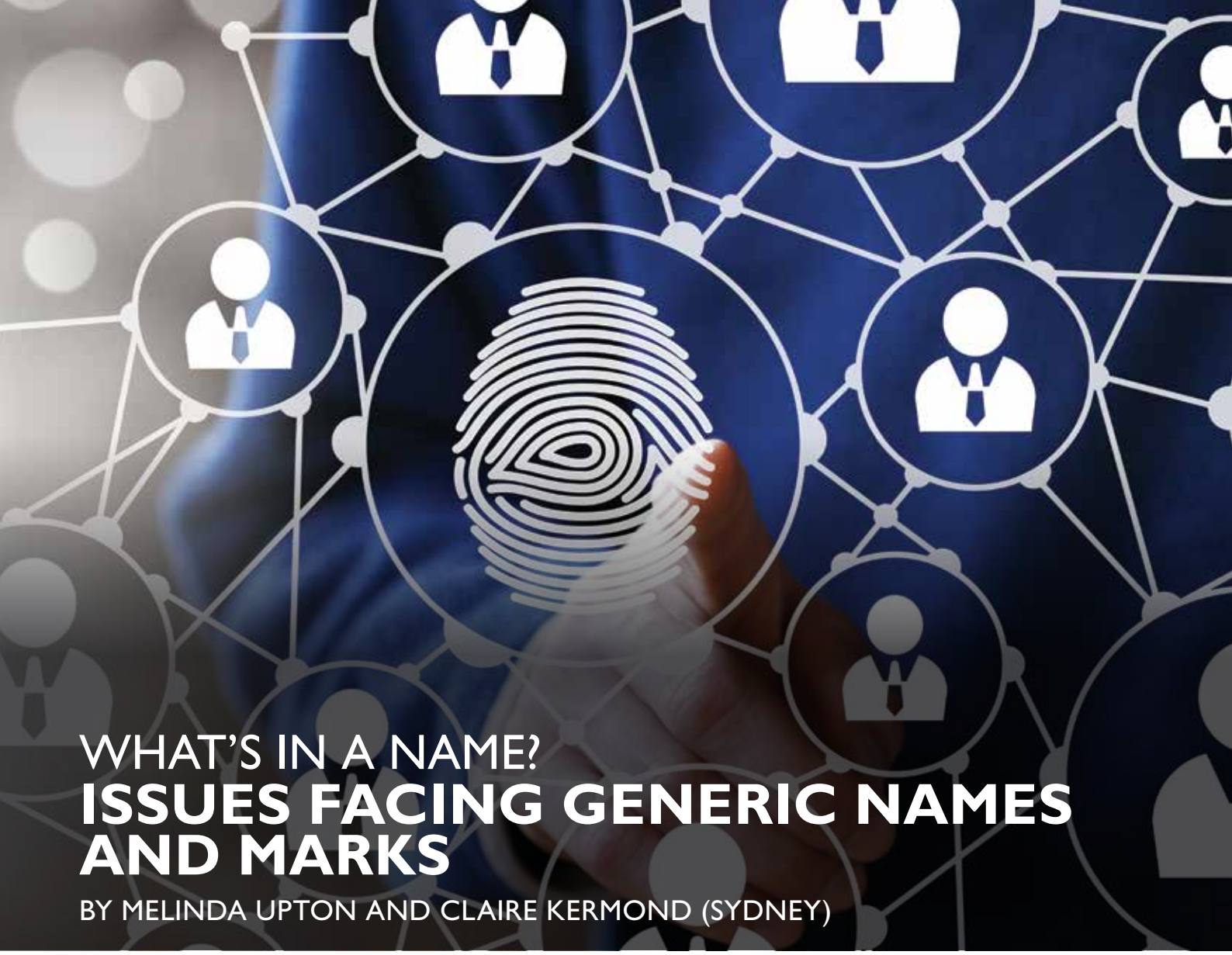
What can you do as a business?

Businesses can take active steps to combat counterfeits, though registration of IP rights, investigations, Customs recordals, and enforcement action such as cease and desist letters and litigation.

But businesses can also take pre-emptive steps to reduce the risk of infringement through appropriate controls and security in design and marketing, as well as the manufacturing and distribution process, at least to make yourself a hard target for counterfeiters.

How we can help you

As a global law firm, we can assist you with the registration and enforcement of your intellectual property rights, as well as advice on processes and commercial arrangements, which make things as difficult as possible for counterfeiters, and make it easier to locate and identify fakes.



WHAT'S IN A NAME?
ISSUES FACING GENERIC NAMES AND MARKS

BY MELINDA UPTON AND CLAIRE KERMOND (SYDNEY)

In the retail and fashion industries, names and marks are a key element of the marketing strategies and longevity of brands. Using generic marks or names can land retailers and fashion designers in trouble when it comes to successfully trademarking and protecting their brand.

Generic marks routinely face certain issues when being registered as trademarks. Indeed, marks that are merely descriptive of the goods and services covered by the application are often refused registration. Fashion designers and celebrities can also encounter the same issues when using their name as a brand or to market a product, particularly when their name is already associated with a well known public figure or is a common name and not unique in the eyes of the Trademark Office.

Kylie Jenner faced these issues when applying to register KYLIE JENNER as a mark in the United States. Her application was refused registration by the US Patent and Trademark Office due to a likelihood of confusion with a prior mark for KYLEE. Jenner recently filed an appeal with the Trademark Trial and Appeal Board over the refusal.

This is not the first time Jenner has had issues in successfully trademarking her name. The artist Kylie Minogue, who owns US trademarks for her perfume, Kylie Minogue Darling, and has used the name KYLIE in relation to jewelry, in addition to her entertainment products, was quick to oppose Jenner's application. Minogue argued that consumers were likely to be confused about the source of the goods and services being offered and that Minogue's brand would be damaged if it were associated with Jenner. Ultimately, however, Minogue withdrew her opposition.

When creating a brand identity for a product or a design, retailers and fashion designers should keep in mind that trademarks used in association with their brand should be chosen carefully. For brands and designers who are still garnering reputation this is especially important. The use of a generic mark or a popular name can leave them vulnerable to others using the name for similar products. Strategically selecting a unique name will go a long way in ensuring long-term success of the brand and effective brand management.

BREXIT UPDATE IMPACT ON TRADEMARKS AND DESIGNS

BY DÉSIRÉE FIELDS & DR ULRIKE GRUEBLER
(London & Hamburg)

Although some time has passed since the UK's vote to leave the EU, the full implications of Brexit for trademarks and designs remain unclear. Statements made by EU and UK officials have not changed that position, nor did Theresa May's Brexit speech in January 2017 provide any indication what path the UK may take with respect to **EU trademarks and Community designs**. The UK Government's White Paper entitled "**United Kingdom's exit from and new partnership with the European Union**" published on 2 February 2017 is equally silent on this issue. It is hoped that more clarity will be gained in the coming months after the UK government triggers Article 50 on 29 March 2017.

The factual and legal situation therefore remains unchanged and can be summarized as follows:

The outcome of the referendum has no immediate consequences on EU trademarks and Community designs as the vote itself does not affect the legal position of the UK as an EU member state. EU trademarks as well as Community designs therefore continue to provide the same scope of protection to rights holders in the UK. It also remains possible to apply for new EU trademarks and registered Community designs which extend protection to the UK and there will be no changes for legal proceedings involving EU trademarks and Community designs initially.

There is no doubt that the status of EU trademarks and Community designs will be among the topics covered during the exit negotiations once these begin. As for many other areas, much will depend on the outcome of those negotiations. However, based on current EU legislation, EU trademarks and Community designs would no longer cover the territory of the UK once the UK leaves the EU.

There is a lot of ongoing discussion between stakeholders about the fate of EU trademarks and Community designs. The Chartered Institute of Trademark Attorneys (CITMA) has outlined some of the options that may be chosen. These include The Republic of Ireland Model (where owners of EU trademarks would have the option to create a corresponding UK trademark registration for a limited time period (e.g. five years after Brexit) or when renewing the EU trademark, the Jersey Model (where the UK would unilaterally deem EU trademark to have effect in the UK), the Montenegro Model (where all existing EU trademark registrations would be automatically entered onto the UK trademark register as UK trademark registrations retaining the same scope of protection) and conversion. These are not the only options that exist, and there are also several possible variations. Although not absolutely certain, it is anticipated that the UK will offer the ability to convert an EU trademark or create an equivalent national counterpart for existing EU trademark registrations. Regardless of which option is ultimately chosen, presentations from the German, Norwegian, ex-Yugoslav and US perspective at the CITMA Spring Conference, which took place from 15 March to 17 March 2017, provide hope that the UK will be more than capable of offering brand owners the necessary protection for their existing and future trademark rights and that the UK will continue to be an attractive jurisdiction in which to do business.

Potential impact

If the UK leaves the EU, neither Community designs nor EU trademarks will cover the territory of the UK. It is anticipated that the UK will permit owners of such EU rights to request a conversion of their EU registrations into national UK registrations. Such national UK registrations may also retain the original filing date of the EU rights. Beyond these assumptions, much remains unclear at the moment. Will the UK Intellectual Property Office (UK IPO) simply accept the list of goods and services of the prior EU trademark or will there be a new examination process, as would be the case currently where rights holders decide to convert their EU trademarks into a bundle of national rights?

Which fee structure will be applied for the conversion process? How long will the conversion process take? Will the "new" national UK trademarks be subject to (another) opposition period? The UK IPO may also ask the applicant to either prove the use of their mark in the UK or request that the applicant declare a bona fide intention to use the mark in the UK, as is currently required when applying for an UK trademark. Some concern has also been raised as to whether EU trademarks might become subject to non-use cancellations once the UK leaves the EU.

Owners of EU trademarks and registered Community designs who make use of the national UK filing system will not need to alter their current filing strategies. However, brand owners who have no parallel registrations in place and regard the UK market as relevant may need to reconsider their filing strategies.

Further considerations

The effect of Brexit on legal proceedings involving EU trademarks and Community designs will also need to be clarified during the exit negotiations. Whereas judgments in legal proceedings post Brexit involving EU trademarks and Community designs will no longer be binding on the UK, it will be interesting to see how the scope of protection of already binding judgments with EU-wide applicability is assessed with respect to the UK after the exit.

Actions

- No immediate consequences for EU trademarks and Community designs as the scope of protection of these rights remains unaffected for the time being
- Continue to follow Brexit discussions to learn about a potential conversion process for existing EU trademarks or registered Community designs
- Rights holders with a particular interest in the UK may want to consider national UK applications for trademarks and designs, in particular for their core brands, to avoid uncertainties in upcoming exit negotiations
- Be specific about what is meant by referring to "the EU" when entering into licensing or settlement agreements, by clarifying whether the UK is to be included

The statistics on trademark filing figures for September 2015 to September 2016 recently published by the UK IPO show that brand owners around the globe appear to be adopting a "wait and see" approach when it comes to filing UK trademark applications. Around 63,500 applications were filed during this period. In September 2016, the IPO received 5,390 new trademark applications, representing an increase of around 800 applications compared with around 4,560 trademark applications filed in September 2015. These figures suggest that the IPO has seen a rise of roughly 10% in applications. Considering the potential implications of Brexit on trademark rights in the EU and UK, this increase does not appear to be hugely significant.

We will continue to monitor developments closely and will provide timely updates as soon as the legislative position is addressed by the UK and EU authorities.

Further information and updates can be viewed on our website: https://www.dlapiper.com/en/uk/focus/brexit-legal-impact/overview/

IPT INSIGHTS

The GDPR at your fingertips: our newest app

The EU General Data Protection Regulation, which comes into force in May 2018, will introduce some of the most stringent data protection laws in the world. It is vital for anyone working with customer data to be familiar with its contents.

To help you to do this, DLA Piper has created the Explore GDPR mobile app. Available on Apple and Android devices, it allows you to access the full text of the EU General Data Protection Regulation on the move with DLA Piper's GDPR app. The fully search-able app, which comes in 13 languages, links articles and recitals to show how they are related.

In addition, articles from the GDPR are linked to corresponding articles from the its predecessor, the EU Data Protection Directive 95/46/EC. And with a single tap, the content can be switched between languages including Czech, Dutch, English, Finnish, French, German, Hungarian, Italian, Polish, Romanian, Slovakian, Spanish and Swedish.

Find out more about the GDPR >>

Australian Consumer Law Review

On 19 April 2017 the final report of the Australian Consumer Law Review, conducted by Consumer Affairs Australia and New Zealand, was publically released. The review was initiated in mid-2015, and involved a broad ranging review of the Australian Consumer Law (ACL) to assess the effectiveness of the provisions and protections and make any recommendations.

The report contains a number of proposals and recommendations which, if accepted by Commonwealth, State and Territory consumer affairs ministers and legislated, have the potential to effect a range of organisations including retailers, life insurers and consumer products/service providers.

Some of the key legislative proposals in the report include:

- A new general safety provision requiring products to be tested by traders for safety. This would be supported by a penalty regime for breaches of the new safety provision, plus expanded ACCC powers to obtain information about product safety
- Clarification of consumer's rights to refunds/replacements and what constitutes a 'major failure', including clarifying where repeat defects or failures together constitute a 'major failure'
- Obligations to make additional disclosures to consumers when offering extended warranties for goods and/or services or warranties against defects
- The addition of a definition of 'voluntary recalls', and an increase in penalties for failure/refusal to notify a voluntary recall
- The extension of unconscionable conduct protection to apply to publically listed companies
- An expansion of the unfair contracts regime to include contracts regulated by the Insurance Contracts Act 1984
- Increasing the threshold in the definition of 'consumer' from $40,000 to $100,000, noting that this would not apply retrospectively
- A tightening of unsolicited selling provisions, specifically around public places, false bills, and where a supplier has obtained a consumer's details from a third party
- Increasing transparency in pre-selected pricing options in online shopping and ensuring that consumer guarantees apply to all online auctions
- An increase in maximum financial penalties for breaches of the ACL, effectively aligning the penalties in the ACL with those in other parts of the *Competition and Consumer Act*. The proposed maximum penalties for companies would be the greater of (a) $10 million or (b) three times the value of the benefit received by the company from the act/omission or (c) if the benefit cannot be determined, 10% of the annual turnover of the company in the previous 12 months

It will be interesting to see how the Commonwealth, State and Territory governments respond to the report and we will continue to monitor those responses and keep you abreast of follow up actions.

WHAT'S ON

TechLaw

- Melbourne 22 June 2017
- Sydney 2 August 2017

DLA Piper will be hosting the annual TechLaw conference in Melbourne and Sydney. This year our keynote speaker, from Deloitte, will present on Deloitte's TMT predictions for 2017. These predictions reveal the perspectives gained from hundreds of conversations with industry leaders, and tens of thousands of consumer interviews across the globe. The predictions identify critical inflection points that inform industry strategic thinking, and explain how these will manifest over the next 12-18 months for companies in TMT, and other industries.

If you are interested in attending these seminars, please contact events.australia@dlapiper.com.

Intellectual property webinar series

Throughout 2017 DLA Piper will be hosting an intellectual property webinar series focusing on the following topics. If you are interested in joining these webinars contact events.australia@dlapiper.com.

- intellectual property issues in China
- confidential information and trade secrets: global insights, global protection
- grey market: parallel importation and anti-counterfeiting
- content protection and digital piracy
- advertising and marketing

Pre-order your copy of the inaugural edition of DLA Piper's Asia-Pacific Trademark Guide

We will soon be releasing the DLA Piper Asia Pacific Trademark Guide, a comprehensive review of trademark laws and key tips covering these 18 countries: Australia, Cambodia, China, Hong Kong, India, Indonesia, Japan, Korea, Laos, Macau, Malaysia, Myanmar, New Zealand, Philippines, Singapore, Taiwan, Thailand and Vietnam.

Covering the complete brand life cycle, this user-friendly guide provides practical insight into key aspects of trademark law and practice in Asia-Pacific, including:

- trademark filing and prosecution
- oppositions
- revocation, invalidation and cancellation
- trademark enforcement
- trademark exploitation
- unregistered trademark rights
- domain and company name disputes.

To pre-order your copy of the inaugural edition of DLA Piper's Asia-Pacific Trademark Guide, email APACTMGuide@dlapiper.com.

Are you an in-house lawyer? Join WIN today!

WIN is our award-winning series of events, tools and forums addressing the technical, commercial and personal aspects of working in-house. Our online community provides access to tailored information, a personal library, best practice guides and toolkits, and extensive selection of recorded webinars, a range of online tools and much more. Click here to register.

EVENT REPORT

ANZIIF InsurTech, Sydney 28 March 2017

DLA Piper was recently a sponsor for ANZIIF's inaugural InsurTech Conference in Sydney. The conference was attended by more than 250 delegates from start-ups through to insurers, underwriting agencies and brokers.

This was a great opportunity to showcase the firm as thought leaders in the emerging area of InsurTech, which is relevant to our key sectors of insurance and technology, as well as networking with many people who are interested in this emerging area. Representatives from some of our key clients were in attendance including **IAG** and **Suncorp**. Our team also had the opportunity to meet key players in this space from the likes of **Data Republic** and **Flamingo**.

Cyber Insight Series, Singapore and Hong Kong

Following on from similar successful events held in Australia last year, our Asian counterparts have held expert panel discussions on cyber risk. On 15 February 2017, our Singapore office held the first instalment of the Cyber Insights Series jointly organised by Aon and DLA Piper. The second instalment was held on 16 March 2017, in the Aon Hong Kong offices.

The moderator of the panel was Murray Wood, Regional Head of Financial Specialties, Aon Risk Solutions, Asia. The first panellist, Paul Jackson, Managing Director, Stroz Friedberg (a recently acquired Aon company) spoke on the security perspective; Scott Thiel, Partner from DLA Piper's Hong Kong office and IPT lead spoke second on the legal aspects of cyber risks; Peter Shelford, Thailand's Country Managing Partner and Co-Chair Insurance Sector, EMEA and Asia Pacific spoke third on the legal and insurance aspects; and finally Andrew Mahony, Regional Director, Financial Services & Professions Group, Aon Risk Solutions, Asia spoke on the risk perceptive. After the panel, attendees were able to ask questions. The event was following by drinks and canapés for a networking and mingling session.

Both events were well attended by approximately 55 people, mostly senior representatives from multinational companies such as AIA, Hopewell Holding, Airport Authority Hong Kong, Hutchison, HSBC and Banco Santander.

International Symposium on Personal Data Protection and Credit Reporting, Beijing 20–21 April 2017

Scott Thiel, Asia Head of Data Privacy, Information Law, Cyber Security and Technology, had the privilege to be invited by The People's Bank of China; APEC Business Advisory Council; and International Finance Corporation, World Bank Group to speak and share his insights at the International Symposium on Personal Data Protection and Credit Reporting held recently in Beijing.

Scott focused his speech on the latest updates regarding data privacy regulatory framework in the Asia Pacific region, current threat environment and enforcement trends, the GDPR (General Data Protection Regulation in the EU) effect, and key challenges and practical issues for multinational businesses.

The symposium served as a platform for foreign practitioners to share the issues they are facing, and the development needs they foresee. They are meant to serve as reference for their counterparts in China. The 2 day event was very well attended by over 100 representatives from People's Bank of China and some other global organisations.

Privacy Awareness Week Update: Industry Debrief: Mapping the community's privacy expectations

On 15 May, our IPT team attended the Industry Debrief: Mapping the community's privacy expectations presented by the Australian Information and Privacy Commissioner, Timothy Pilgrim and Principal from The Wallis Group, Jayne Van Souwe.

We heard some of the key issues raised by the *2017 Australian Community Attitudes to Privacy Survey* and part of the Office of the Australian Information Commissioner's (**OAIC**) plan to address rising privacy concerns in Australia. It was also notable that the survey confirmed many Australians being comfortable with and welcoming the new mandatory data breach notification rules due to come into effect early next year.

Survey findings:

- 83% of all Australians viewed online interactions are inherently more risky in privacy terms (although many privacy breaches that the OAIC currently handle are offline and low tech).
- 25% never ask why their personal information is being collected.
- 9 in 10 Australians are concerned about personal information being transferred overseas and confirm they do not like it.
- 79% are uncomfortable with sharing their data in a commercial sector.
- Young Australians under 35 are the most likely to exchange data for benefit.
- The health sector continues to be regarded as the most trustworthy, with financial institutions and government sector following closely behind.

Some notable key points:

- there is a considerable gap between privacy concern and actions of all Australians;
- consumer's decision making relies on existing goodwill and trust in an organisation over detailed policies – for example: many Australians are not likely to read a long and complex privacy policy; OAIC confirming that simplifying privacy policies will be a core focus; and
- there is significant personal responsibility in personal information protection. Everyone has a role to play.

The Commissioner, Mr. Pilgrim, highlighted some actions the OAIC has recently undertaken and some currently in progress, including:

- working with CSIRO to develop tools to assist with de-identification of data and information – the OAIC posing the question "Can you really de-identify personal information?";
- preparing the OAIC response to the *Productivity Commission report on Data Availability and Use* that was released last week;
- working with the Prime Minister's public data groups to establish how data can be used for "good purposes" and how to avoid the impact on individuals – in line with a trend towards open and effective use of data;
- exploring the social/economic use of personal information – a possible social licence for innovative data use, including options of notice and consent;
- their recently published their guide to "personal information" on the OAIC website;
- soon to be released the final *Australian businesses and the EU General Data Protection Regulation* guidance within the next coming weeks see the draft resource here – according to the Privacy Commissioner, the GDPR is "extraordinarily important" to Australian businesses; and
- educating Australians about the Right of Access to personal information, indicating a potential focus point on data subject access right here also.

www.dlapiper.com