DLA PIPER

ASIA PACIFIC

INTELLECTUAL PROPERTY AND TECHNOLOGY NEWS

Perspectives • Analysis • Visionary Ideas

NOVEMBER 2015

www.dlapiper.com

IN THIS ISSUE...

EDITOR'S COLUMN

Welcome to the latest Asia Pacific Edition of 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.

With the end of the year fast approaching, an emerging focus discussed in the media more and more frequently is Internet of Things (IoT), which has important social, economic and legal implications. IoT will dramatically change business and business models, affecting the way consumers access businesses, and the way businesses gather information.

IoT is an important area of focus for the Intellectual Property and Technology team, and this issue will explore the things you need to know about IoT from a legal perspective.

While IoT technologies offer the prospect of efficiencies, productivity gains and savings in costs and resources, there are many risks. Chief among these are concerns regarding data privacy, and the loss or leakage of personal data. Both will be explored in more detail.

Data analytics continues to be in the spotlight, with more and more focus being placed on the significant amount of digital information collected by businesses. This issue will explore how such data can be used to benefit the organisation and its customers, and how data analytics fits into the field.

Meanwhile in China, major changes to advertising laws have been enacted to increase the protection afforded to individuals and businesses. This issue will focus on the key provisions of the Existing Law and the key amendments introduced by the Amended Law.

Companies in Asia are generally considered as less prepared for the increasing number of cyber crimes than counterparts in other regions. This issue will provide tips for employers to help avoid cyber risks and fraud.

We hope you enjoy this issue of IPT News. Please feel free to provide us with any suggestions, questions or feedback that you may have so we can continue to make this a publication you look forward to reading.

Kind regards

Melinda Upton
Head of Intellectual Property and Technology Group Australia
melinda.upton@dlapiper.com

Ann Ford
Global Co-Head of Sectors
US Head of Sectors
Chair, Trademark, Copyright and Media Practice
Vice Chair of Intellectual Property and Technology Group US
ann.ford@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/.

THE TOP SIX THINGS YOU NEED TO KNOW ABOUT INTERNET OF THINGS: A LEGAL PERSPECTIVE

By Peter Jones, Partner (Sydney), Tim Lyons, Partner (Melbourne), Sharon Rowe, Partner and Anna MacFarlane, Senior Associate (Canberra)

IoT is discussed in the media more and more frequently. It has important social, economic and legal implications, most of which are yet to be fully understood.

The following sets out a brief list of things you should know about IoT from a lawyer's perspective.

1. IoT is here and it's changing the way we live and interact with each other. It will change the way consumers interact with suppliers, businesses interact with their employees and each other and government interacts with its customers, employees and contractors.

2. IoT is about smart 'things', which record and transmit data automatically via the internet and without the need for human input. Examples include:

- Fridges that record when you are out of milk and which purchase milk online from a supermarket for you.
- Watches that record your heart rate, movement and sleeping patterns and send that data to your smart phone for your review or even to a medical monitoring service.
- Building access cards that automatically report to your employer that you are late for work and then set your out-of-office email notice for you when you leave.
- Bathroom scales that record and send your weight readings via wi-fi to an app on your phone.
- Sensors used in industrial control systems for utilities to predict the maintenance required to provide services to you.

3. IoT could be used to monitor and report on an endless number of compliance and risk issues in the workplace and at home. For example:

- What if your wearable activity tracker provided information on stress levels to your employer?
- What if your car could report to your insurance company that you are a bad driver and your insurance premium increases?
- On the plus side, IoT can also be used to make life simpler. For example:
- If you are in an accident, what if emergency assistance was immediately called (if needed) and insurance claims automatically lodged?
- What if your bin could put itself out when the truck is approaching and the toilet seat could put itself down for select members of the household? Would this completely eliminate marital disharmony?

4. IoT products automatically collect and transmit data on a scale that we have not seen before. Both suppliers and purchasers need to carefully consider contractual provisions and protections when selling or purchasing IoT enabled products, or incorporating IoT solutions from third parties into their products. What about the telecommunications providers? Where numbering and spectrum are increasingly scarce, and networks configured for specific data types, how will IoT be enabled (and who will pay)?

5. IoT also gives rise to significant data protection and privacy issues. How the data is collected, transmitted, stored and used is critical, as anyone who can access it will be able to gain an intimate view of almost all aspects of your life. Will the regulatory framework be able to accommodate IoT? Will privacy become more or less important to us in an IoT saturated world?

6. IoT also gives rise to a myriad of other legal issues, including security, IP and product liability issues. For example, what if your IoT fridge orders too much milk or your IoT medical monitoring watch malfunctions and calls an ambulance every hour (or worse, not at all)? Who should bear the legal risk? Will this be covered by our household or corporate insurance policies?

The opportunities from IoT are limitless, and DLA Piper is proud to be one of the legal thought leaders in this space. DLA Piper will soon be holding a number of IoT events nationally, as well as continuing to issue publications on this topic. To register your participation in our DLA Piper IoT interest group, please click here.

Balancing convenience and risk: The Internet of Things for business

Peter Jones, a partner in our technology team has recently spoken to BRR media about the impacts of the IoT and explains the legal implications.

Watch now

INTERNET OF THINGS: Asia

By Ed Chatterton, Partner, Scott Thiel, Partner and Louise Crawford, Legal Officer (Hong Kong)

Cybersecurity and the protection of personal data should be the key focal points in Asia over the coming years, as the region is poised to see a rise in technological advancements, and the increasing prevalence of the IoT. Software is gradually falling out of vogue to be replaced with hardware, robotics and IoT devices. In Hong Kong, for example, there has been huge investment in this industry. Andrew Young Meng-Cheung, Chief Commercial Officer of the Hong Kong Science and Technology Park, has said that Hong Kong is "moving in three directions: robotics, healthy ageing, and smart city."

Of particular interest in the Asian market is the development of technology to assist with geriatric care, due to the ageing population, and the cultural trend in many Asian countries for people to care for their parents. Similarly, there is increasingly a move to 'smart cities', with Singapore, Bangkok and Jakarta launching initiatives to use technology to improve lives and businesses, ranging from transport maps and apps to make travel easier, to connected homes to control lighting and air-conditioning via tablets and smartphones. IoT is also expected to drive an uptake in smart education and personalised learning through the use of information technology.

Predictions for Asia

- The International Data Corporation forecasts that IoT in Asia-Pacific (excluding Japan) is set to explode to 8.6 billion devices by 2020, growing from a current annual market of US$250 billion to US$583 billion in 2020.
- It has been predicted that the size of the consumer technology market in China, the world's second largest economy, will grow by about five per cent to US$281 billion in 2015, likely overtaking the US as the primary market for consumer technology goods.

- The Malaysian Ministry of Science, Technology and Innovation (MIMOS) launched the National Internet of Things (IoT) Strategic Roadmap in July 2015, to drive the adoption of IoT. This is expected to contribute US$2.49 billion to the country's gross national income by 2020.
- In a recent PricewaterhouseCooper study, respondents from Asia were most likely to say that their companies are investing in sensors (key IoT technology), followed closely by Latin America.
- Oordeoo and Ericsson recently launched IoT initiatives in Indonesia.

Key considerations for IoT in Asia

In addition to advances in low-cost hardware, connectivity, and software, achieving the full potential of IoT in Asia will require improvements in security and sophisticated methods for ensuring privacy, protection of intellectual property, and assignment of data ownership. As IoT application touch on so many areas of regulatory and government responsibility, policy makers will play a key role in enabling IoT in Asia. To take full advantage of IoT, policy makers will be required to help by addressing concerns about security and privacy and encouraging the development of standards to promote interoperability.

Security

Cybersecurity has become a top-tier risk for all multinational organisations. As Cisco CEO John Chambers recently predicted, the volume of cyber attacks and, ultimately, the number of successful penetrations, is likely to increase exponentially.

Attackers innovate rapidly at little expense, harnessing sophisticated cyber weapons, sharing techniques and 'renting access' to corporate networks to less sophisticated cyber criminals. Hackers typically operate beyond the reach of developed world law enforcement and are almost never apprehended.

In this area, many countries in Asia-Pacific are arguably behind the pace, with some countries only now introducing cybersecurity strategies and other countries having no strategy in place. A recent study by The Software Alliance (BSA) and security market researcher Galexia, which evaluated 10 countries in Asia-Pacific on five key aspects of cybersecurity, found that China, South Korea and Indonesia were hindered by local standards and testing requirements. South Korea, Malaysia, China and Vietnam were still in the process of developing their cybersecurity infrastructures, whereas Indonesia had no cybersecurity plan to speak of. The study identified Singapore as the clear leader in cybersecurity, flagging Singapore's 2013 5-Year National Security Plan and the establishment of a new Cyber Security Agency which has oversight of Singapore's cybersecurity functions. Identified as key was the fact that the Singapore government was also committed to developing public/private partners to improve cybersecurity.

To take full advantage of IoT, governments in Asia-Pacific would be well-advised to follow Singapore's lead in the development and implementation of a national cybersecurity plan, the establishment of independent bodies to oversee national cybersecurity functions and introduction of public/private partners to improve cybersecurity.

Privacy

Asia-Pacific's 'report card' is arguably far stronger with respect to the protection of personal information with Singapore, Malaysia, the Philippines, South Korea and Taiwan all recently introducing comprehensive data protection regimes in their respective jurisdictions. These follow the long-standing data protection regimes in Australia and Hong Kong, both of which have recently further strengthened their regimes. There are clear data collection guidelines applicable in Asia to companies and public bodies. However, even here, Asia-Pacific is still playing 'catch up' with other jurisdictions. What is becoming increasingly clear is that the increasing connectivity of devices, and the resultant data flows between those devices, will make it harder for businesses to comply with data privacy legislation. The key issues identified include lack of informed consent from the consumer to such data flows and the increase in connected devices multiplying exponentially the amount of data that can be accessed and analysed. As they play catch-up with more established regimes elsewhere, the regulators in Asia-Pacific will need to play a careful balancing act between the right to privacy in personal data and encouraging the adopting of IoT, with all of the benefits that it can bring.

INTERNET OF THINGS: GENERATING OPPORTUNITY BEHIND THE BUZZ WORDS IN THE ENERGY SECTOR

By Jane Collis, Solicitor (Brisbane)

No longer a buzz word, the reality of IoT is demanding attention in 2015. It is predicted that businesses who embrace these opportunities will transform not only their business but also their industries along the way. The energy sector is not immune.

How are companies in the energy sector currently deriving value from IoT and where might additional opportunities lie moving forward?

Financial performance

A lot of early investment into IoT technology has been focused on finding new ways to reduce the bottom line.

Smart hardware has been installed to manage a broad range of assets and to facilitate a number of industrialised tasks. Equipment and vehicles have been retrofitted with sensors which can feed data to personnel who can assess and diagnose problems quickly and remotely. Sensors have also been able to harvest useful data in relation to the utilisation of particular equipment or vehicles including data relating to performance and breakdown, maintenance requirements and demand to allow better scheduling and use of workforce and resources.

However, the ability to harvest massive amounts of data also provides an opportunity to gain insight into the demand side of the equation and identify new ways to drive top-line revenue growth. This may be identifying opportunities to deploy IoT technologies in new ways, identifying opportunities to meet previously unmet needs and demand or identifying poor performing products, services or processes and refocusing investment into those which will derive more revenue growth moving forward.

Operating performance

Energy companies have been using IoT technologies for the purpose of incrementally optimising the performance of its assets and resources.

Data analysis tools have been developed which generate real time data visualisation for smartphone and tablet applications. Adoption of this technology has resulted in meaningful increases in profitability as access to immediately available data creates greater opportunities to optimise processes, reduce downtime by addressing variances quickly before they lead to abnormal operations, shutdown and equipment damage and create safer environments through incident prevention.

The opportunities to drive better performance may well extend beyond incremental asset and resource productivity. By installing and connecting sensors, companies can now monitor how customers and stakeholders engage with products and services on a day to day basis and harvest that information to identify and drive improvements in performance, increase value to their customers and stakeholders and tackle issues that customers and stakeholders experience.

The smart grid market is a great example of IoT technologies being harnessed to drive better performing products and services. The network of sensors and connected technologies will enable power companies and nations to deliver more efficient and reliable power supplies all while reducing the environmental and cost impact of the energy system.

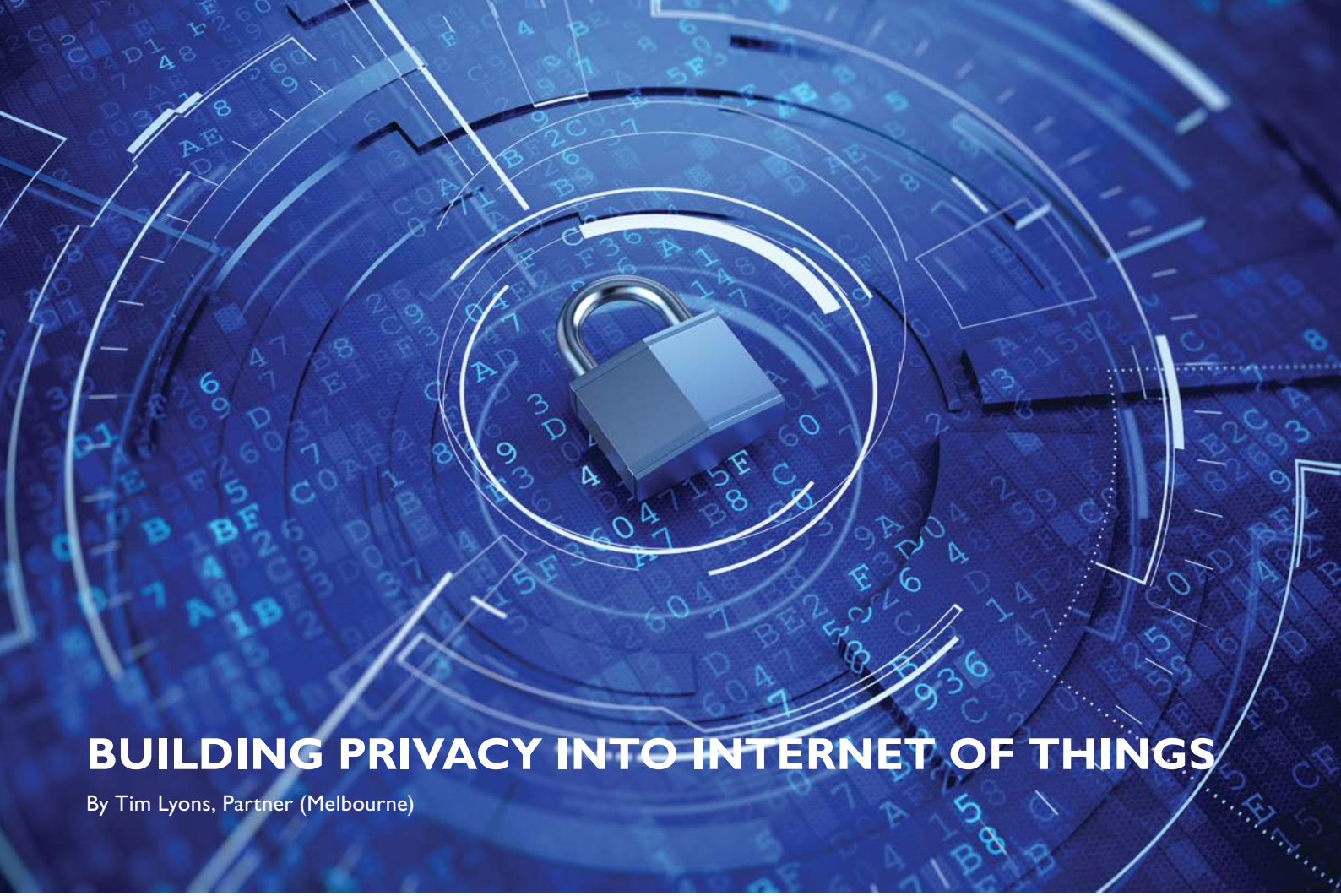
There has been much less attention on the potential benefits that may flow from systematic monitoring of performance over time. The performance related data collected over time may be able to be harnessed to drive more fundamental changes to the core business. By monitoring and analysing the overarching performance of the company, greater insights may be gained in relation to efficient and inefficient processes, environments and structures.

Challenges

The possibilities created by IoT has captured the imagination of the energy sector. However, business leaders are faced with the task of balancing the adoption of new (and often disruptive) technologies and innovations with operational realities and the regulatory landscape.

Key issues facing companies seeking to embrace IoT, include:

1. Cybersecurity: Connecting so many things and processes to the internet comes with a huge cybersecurity risk. Cybersecurity technologies, the right policies and carefully thought out contractual protections are all required to address this challenge.
2. Privacy: Ensuring compliance with privacy and data protection laws is complex in connected environments where data is shared, analysed and accessed between business functions, machine to machine and by third party vendors.
3. Liability: Greater reliance on technology and machine to machine processes creates complex questions regarding who is liable for system defects and failures, security breaches and unintended consequences.
4. Dependency on technology and risk of failure: As organisations become more reliant on technology, it is vital that risks associated with dependency, including technology breakdown, technology incompatibility, vendor insolvency or vendor relationship breakdown, are appropriately mitigated against.
5. Access to capital: With many parts of the energy sector facing shrinking capital markets, it is often difficult to find the resources to invest in adoption of IoT enabled technologies or create a strong business case for being a market leader in this space.
6. Network coverage: Poor network coverage and access to bandwidth remains an issue in some remote and regional areas.



BUILDING PRIVACY INTO INTERNET OF THINGS

By Tim Lyons, Partner (Melbourne)

IoT: Extending the internet into things

IoT refers to the extension of the internet into the physical world. In the IoT, the internet connects not only personal computers, tables and other 'smart' devices but also 'dumb' objects such as toasters, sofas, shoes, light bulbs, aeroplane wheels, cattle and human bodies. While IoT technologies offer the prospect of efficiencies, productivity gains and savings in costs and resources, there are many risks. Chief among these are concerns regarding data privacy.

Data privacy in the consumer IoT

Like all technological developments, IoT is open to many different uses and the potential consequences for the consumer are profound. For example, employers, insurers, lenders and others could make important decisions based on inferences drawn from data generated by IoT technologies without regulators having much understanding of the process. Consider activity trackers (such as the ubiquitous Fitbit): a prospective employer could request data generated from such devices to seek to predict a prospective employee's efficiency and productivity using data on sleeping and exercise patterns and the setting and achieving of goals. In the home, connected televisions and other media consoles can reveal the type of content a person consumes, be it news or cartoons. Likewise, an internet-enabled couch and floor could determine how often a person is sedentary, leading to inferences about a person's motivation and/or health.

Addressing privacy concerns: A question solely for regulators?

Much has been written about the application and potential shortfalls of data privacy laws in the context of the IoT. Legal protection of data privacy is obviously essential, and legislators and regulators around the world are grappling with how to best provide sufficient protection for consumers, and useful guidance for IoT developers, without stifling innovation.

Given the rapid rate of technological development in the IoT it may be that legislation and other regulatory guidance develops into a general (but useful) framework for IoT developers to operate in, rather than a step-by-step guide for data privacy compliance. Indeed, while the law sets certain standards for data privacy, when dealing with technology it can be difficult for legislators and regulators to be too specific, given the rate of change. Aside from any legal compliance, many consumer technology providers instinctively understand the importance that consumers place on the protection of their personal data. These providers are actively seeking to strike the right balance between leveraging the great insights that can be gleaned from personal data generated in IoT and building consumer trust through privacy enhancing applications.

Therefore, the key question now emerging is how do IoT providers meet data privacy expectations and legal requirements, not why they should be seeking to do so.

Privacy by Design in IoT: A refocus on 'the user'

Privacy by Design (PbD) refers to the process of building privacy enhancing mechanisms into the design of technology, as opposed to considering such mechanisms as an afterthought. Originally conceived by regulators, PbD holds that the future of data privacy cannot be assured solely by compliance with regulatory frameworks. The current Victorian Privacy Commissioner Mr David Watts has said that: "at a high level, what Privacy by Design mandates is embedding privacy into the information technologies, business practices and networked infrastructure, as a core functionality, right from the outset".

PbD is arguably crucial to privacy enhancement and legal compliance in the IoT given the difficulties presented by new IoT technologies. For example, it may be difficult to obtain meaningful consent from individuals to the collection of personal data through certain IoT devices that do not have traditional user interfaces, such as a connected utility meter. Similarly, it may be difficult to provide sufficient data collection notices to consumers using devices like internet-enabled floor tiles or coffee machines.

Much of the guidance on how to implement PbD issued by regulators and the private sector is often very general, out of date, and, at times, assumes that data security is the same as privacy or conflates the two issues. In the absence of clear guidance, technology developers are struggling to meet the key requirements and outcomes of data privacy as distinct from security, which is often their native area of expertise.

In recent times, some developers have turned to a tried and tested but, as yet, largely overlooked approach to solving these issues: a focus on the user. While security engineers are needed to build secure systems, software developers are needed to address key data privacy issues in software and hardware specifications, and lawyers are needed to ensure compliance with the law, a key division is often overlooked: user experience designers (UX). UX designers specialise in improving the aesthetics, ergonomics and usability of products and services.

In placing the user experience at the heart of technology products and services, the consumer technology market has been transformed. Utilising UX design principles, IoT developers may approach data privacy compliance in a similar way. Examples of UX data privacy include data 'featureisation', which is the practice of making data a consumer-side feature of products and services, building systems that allow users to access their data in an easy, usable format while providing mechanisms that place a value on the sharing of data, and developing tools that permit providers to obtain real, meaningful consent to data collection and use.

IoT providers must tell their UX designers to take privacy considerations in account in the same way as they take into account aesthetics, ergonomics and usability when developing products and services.

MOVING FROM 'BIG' TO 'RELEVANT' – THE IMPORTANCE AND CHALLENGES OF DATA ANALYTICS

By Peter Jones, Partner (Sydney)

The term 'big data' is one which is now in almost common use in many organisations and the world of business generally. While the term means different things in different contexts, in this article (and at its most basic), it refers to the significant amount of digital information collected by businesses from their provision of products and services to customers and the subsequent use of those products and services by customers together with other sources of data (for example, publically available data sets; data sets available from third party suppliers).

The question that then arises is how can such data be used to benefit the organisation and its customers? This is where data analytics enters the field.

There are many areas in which broad and detailed data sets can potentially provide incredibly useful insights to organisations, such as:

- the undertaking of more effective marketing of products and services through tailoring to specific customers, for example by identifying certain categories of customers where data analysis suggests such customers are more likely to accept specific product/service offers than other categories.
- the development of new and better products and services, increasingly tailoring these to the individual customer with the aim of providing greater convenience and closer links to the customer.
- the identification of longer term trends, enabling earlier preparation for potential strategy adjustments or more radical changes.

To do this though, there is a need to convert large quantities of data, through qualitative analysis, to provide relevant business insights. In short, data analytics results in the visualisation of previously unidentified correlations and patterns. Further, as significant amounts of data is often based on convenience samples or subsets, analysis is required to adjust for any biases, to remove 'false positives' (where the data suggests a specific causative effect which on closer examination is false) or to provide missing context.

For example, I argue that Sir Richard Hadlee is one of the best bowlers in test cricket of all time. Using available statistical data such as bowling average, the number of wickets taken, the average number of deliveries required for each wicket and the average number of wickets taken per test, there is a strong argument. However, the fact that he played a significant number of tests at home in New Zealand at a time when the wickets greatly assisted bowlers is also relevant. As is the fact that some of the New Zealand slip fieldsmen were undoubtedly very good. Also, the overall calibre of batsmen for the decade or so following the late seventies, with the probable exception of the West Indies, was weaker than the overall calibre of batsmen from 1995 onwards (Lara, Tendulkar, Ponting etc). So, analysis is not an easy task.

Data analytics in the context of big data also raises a number of legal and risk issues.

First is, unsurprisingly, privacy considerations. To the extent that relevant data is personal information for the purposes of relevant privacy regimes, compliance with applicable regimes will arise and can significantly impact on the ability to undertake data analytics (for example do... privacy consents contemplate such a use? Do consents effectively provide for third party suppliers to undertake services on behalf of the data collector? If cross-border access/disclosure is contemplated, what requirements arise?)

A related issue is whether the use of anonymised data or specific items of data which are not themselves 'personal' is sufficient to fall outside privacy parameters. This is an issue privacy regulators are facing and will increasingly face, and the answer is not necessarily simple. For example, a recent decision by the Privacy Commissioner in Australia held that information such as IP addresses and specific cellular tower was personal information of a consumer of telecommunications services because of the ability of the service provider to aggregate that data with data in other systems which provided the necessary personal identification. Note the service provider is reviewing this decision given its potentially wide impact. With a trend towards privacy regimes including substantial requirements and penalties for non-compliance such as mandatory notification of data breach; significant fines; and, in some jurisdictions, imprisonment, the impact of privacy regimes cannot easily be avoided.

Further, could an organisation's use of data analysis to provide specific products or services, or specifically priced products or services to some categories of consumers and not others, lead to claims actionable under anti-discrimination laws? If so, do any statutory or other exemptions apply (for example, discrimination legislation may allow insurers to act in a manner that would otherwise result in a breach based on actuarial or other statistical data – what standard is required to meet any such exemption)?

Also, data security considerations arise. While data security and cyber-resilience are matters for all organisations, if a third party data analytics provider has been engaged and personal information or confidential information is required to be (or more likely is inadvertently) provided, and then is subsequently disclosed by or accessed from that service provider, what legal or contractual obligations apply to the third party? How is risk allocated under the relevant contract?

Finally, what impact does the use, or potential misuse, of data analysis outputs have on an organisation's reputation/brand? This issue overlaps with some of the legal considerations set out above – an organisation being held liable for a failure to comply with legal obligations is rarely brand enhancing. But for boards and senior executives, this is a much broader and potentially more damaging issue as well. As organisations move to increasing categorisation/targeting of their customer interactions, and differentiated products, services or processes are provided, one person may see convenience; another may see inappropriate business over-reach. In this respect, gauging when and how to use data analysis is a significant, and ongoing, challenge.

CHINA ENACTS ITS FIRST MAJOR CHANGES TO ITS ADVERTISING LAWS IN TWENTY YEARS

By Edward Chatterton, Partner, Ian Jebbitt, Senior Associate (Registered Foreign Lawyer) (Hong Kong)

When will things change

The existing PRC Advertising Law (Existing Law) entered into force on 1 February 1995 and has not been amended since then. With the advance of the internet and the fact that the average person is now reported to spend almost two hours per day on social media, the advertising landscape has shifted dramatically. Legislators all around the world, not just in China, are playing catch up. The amendments to the Existing Law seek to modernise the legal framework surrounding advertising and address issues which exist in modern day China that could not have been foreseen 20 years ago, when the Existing Law was introduced.

The amended PRC Advertising Law (Amended Law) was officially approved on 24 April 2015 and came into force on 1 September 2015. The Ministry of Industry and Commerce has wasted no time in enforcing the Amended Law with reports suggesting that smartphone maker Xiaomi is currently under investigation for the use of superlatives in their online ads, which is prohibited under the new regulations.

The Amended Law is part of a bigger picture. China is amending a number of its laws in the branding and marketing space to increase the protection afforded to individuals and businesses in China. The underlying aim behind all of these changes is to demonstrate that China is committed to protecting and safeguarding the rights of individuals and businesses. In May 2014, China enacted a new Trademark Law which introduced some major changes aimed at modernising trademark law in China and reducing trademark piracy, and an amendment to the Copyright Law is currently working its way through the approval process.

The Existing Law is very short and has been widely criticised for being too vague. The Amended Law is almost double in length and is much more prescriptive, with one of the key aims being to reduce the number of grey areas that exist in the advertising space in China, making compliance and indeed the imposition of sanctions for non-compliance, much more straightforward.

This article focuses on the key provisions of the Existing Law and the key amendments which were introduced by the Amended Law on 1 September 2015.

Summary of key provisions of the existing law

The Existing Law provides that advertisements must:

- be true and must not contain false and misleading information which cheats or misleads consumers
- adhere to the principles of fairness and trustworthiness
- not be detrimental to the physical and mental health of the people of China
- not impair the physical and mental health of minors or disabled people
- be in compliance with social morality and professional ethics and safeguard the dignity and interests of the state
- only contain data, statistics and survey findings that are factually correct with the source being indicated in the advertisement
- not discredit the products or services of third parties.

The Existing Law also contains specific restrictions in relation to the advertising of pharmaceutical and medical devices, agricultural chemicals, tobacco and health foods.

Summary of key provisions of the amended law

Misleading advertising

The Amended Law provides specific examples of what will constitute a misleading advertisement and thus provides further detail on the scope of what is otherwise a very broad and un-prescriptive definition. Specifically, advertisements that provide incorrect information in relation to the performance, function, origin, uses, quality, size, composition, prices, manufacturers and expiration dates of products will be considered misleading.

Children

The Amended Law introduces more controls on advertising aimed at children. All advertising in schools and kindergartens is prohibited, as is advertising in textbooks and exercise books and on school uniforms and school buses. Children under the age of 10 cannot be used to endorse products or services. Endorsement is defined as "recommending or providing testimony in support of products or services in an advertisement". Mr. Zhang Guohua, one of the State Administration for Industry and Commerce officials responsible for the enforcement of advertising laws in China, stated in an interview that this provision does not mean children under the age of 10 cannot feature in advertisements; they just must not specifically endorse the products or services being advertised.

Furthermore, advertisements targeting children under 14 must not contain content which persuades their parents to purchase the goods or services being advertised. It is however unclear at this stage what constitutes "content which persuades" but this will hopefully be made clear when the implementing regulations are published later this year. Advertisements targeting children under 14 must also not contain content which encourages the imitation of dangerous acts. The Amended Law also prohibits the advertising of cosmetics, medicines, medical apparatus, online games, alcoholic beverages and tobacco to children.

Communication of advertisements

Advertisements must not be sent to home addresses without prior consent. In addition, other forms of electronic direct marketing are also prohibited unless an individual's consent is first obtained. Any advertisement must also not interfere with people's normal usage of the internet, meaning care needs to be taken when using pop-up advertising. Under the Amended Law, a pop-up advertisement must be capable of being closed in one click. Furthermore, an electronic advertisement must also include the sender's true identity, contact details and information as to how to un-subscribe from receiving further advertisements.

Telecoms

The Amended Law imposes liability on service providers responsible for communicating advertisements which breach the Amended Law if they were aware of the content and did not take action to stop the advertisement.

Product endorsement

Anyone who endorses a product may be held jointly liable for any infringement of the Amended Law if he or she ought to have known the advertisement infringed the Amended Law. Anyone found guilty of endorsing a false advertisement can be banned for endorsing other products or services for a period of three years.

Sanctions

The Amended Law introduces wider ranging sanctions including fines of up to 1,000,000 RMB (circa US$150,000) and the imposition of criminal liability and revocation of business licenses for serious instances of infringement.

Sector-specific amendments

The Amended Law also introduces more stringent control on advertising in a number of specific areas, including the financial services and alcohol and tobacco industries.

Financial services

One of the key sector-specific amendments is in relation to the promotion of investment products. The Amended Law introduces specific requirements that businesses will need to be aware of when promoting investment products. For example, the advertisement of investment products must:

- alert consumers to the risks involved with the product and any possible losses and liabilities they may suffer
- not include any guarantees on future returns unless the returns are 100 percent guaranteed
- not suggest that any capital invested is risk-free unless it really is
- not use the name or image of academic institutions, industry associations, or professionals to give a misleading air of credibility to an investment product

Tobacco and alcohol

There are in excess of 300 million smokers in China and it is estimated that more than a million people die each year in China from smoking-related illnesses. With the recent introduction of wide spread public smoking bans, including in Beijing, greater emphasis is being placed on reducing the number of smokers in China. The Amended Law introduces specific requirements that businesses will need to be aware of when promoting tobacco products. For example, tobacco products:

- must not be promoted in mass media, public venues, public transports, or on outdoor advertisement boards
- must not be promoted as part of advertisements for other products or services or for charitable purposes

There has also been a change in drinking behaviour within the Chinese population. A recent national survey China revealed that of those interviewed; 62.7 percent of the men and 51.0 percent of the women reported excessive drinking; 26.3 percent and 7.8 percent, respectively, reported frequent drinking; and, 57.3 percent and 26.6 percent, respectively, reported binge drinking.

The Amended Law is one of many measures being adopted to try to reduce alcohol consumption in China and, under the Amended Law, any advertisement for alcohol:

- must not promote drinking to excess
- must not show the actual action of drinking
- must not show driving cars, vessels or aircrafts
- must not show that drinking help to relieve pressure, anxiety or tiredness, either expressly or implied

The practical implications of the amended law

The Amended Law shows a definite intent to police advertising more stringently and we believe the authorities will be keen to be seen to be zealously enforcing the Amended Law after it comes into force.

We believe close attention will be given to advertisements of products and services in those areas which the Amended Law has introduced new and wider reaching measures. As such, businesses operating in these industries should ensure they are fully cognizant of the provisions of the Amended Law in these areas and should make any changes to their operational processes that are required to ensure they do not fall foul of the Amended Law.

The Amended Law also introduces much tighter control around online and social media advertising and businesses who engage in this type of advertising in China should review their online and social media operating procedures and guidelines to ensure they comply with the Amended Law.

BE ALERT ASIA – TOP TIPS FOR EMPLOYERS: CYBER RISKS AND FRAUD

By Julia Gorham, Head of Employment Asia and Anita Lam, Of Counsel (Solicitor Advocate) (Hong Kong)

Cyber risk is becoming a growing concern amongst businesses and institutions. Data breaches and hacking have been problematic among some sectors, predominantly financial services, for some time. These risks are now often talked about under the broader heading of 'cyber risk' and this issue is listed as one of the top business risks in 2015. Companies in Asia are generally considered less prepared for the increasing number of cybercrimes than counterparts in other regions like the USA.

When a security breach involves the loss or leakage of personal data, this also becomes a significant data protection and regulatory issue and can lead to fines, legal or regulatory sanction and reputational damage. This is particularly in a market environment where individuals (be they customers or employees) are becoming increasingly aware of their privacy rights and identity theft issues. With the arrival of Internet of Things, the importance of data security will become even more prominent. The consequences of not protecting your business sufficiently from cybercrimes can be huge.

Despite the challenges faced by many companies, some of these risks can be identified and avoided at an early stage. Whilst most companies are aware of the firewalls and technology they need in place to protect themselves, many are unaware of other 'soft spots' that may also be contributing to the risks in a major way.

'Soft spots' include employees who unintentionally open 'phishing' or spam emails, disgruntled or former employees who deliberately take confidential information and other issues that come with Bring Your Own Device (BYOD).

There are ways to deal with these 'soft spots', including improved governance and compliance and training for employees and tighter security solutions. However, a top-down approach is needed and senior management, including board members, need to make cybersecurity a priority.

Top tips in dealing with cyber risks from an employment perspective include:

Governance and compliance

- Identify highly sensitive and classified information, customer and staff data kept by the company.
- Identify ownership of the data (for example human resources department, finance, a specific business team) and the security measures put in place.
- Identify all the data processors used by the company, check which of these data processors are engaged to handle the company's highly sensitive and classified data.
- Identify the legal and compliance requirements in relation to the use and security of data, and the legal and regulatory consequences of a data breach.
- Perform risk assessment: identify those risks where the consequences of data breach are extremely serious. Implement measures to mitigate those risks.
- Roll out policies on data security and use of IT. Consider including it as part of the company's staff regulations.
- Implement the data security and use of IT policy, including taking disciplinary measures, if there is a serious violation of the data security and use of IT policies.

Employee training

Employees need to understand that they have an important role in keeping both the network and the data safe.

- Train employees to watch out for suspicious emails. If it is a hoax, report it.
- Promote awareness: learning is continuous, as cybercrime can manifest itself in many different ways.
- Instil information security behaviour that affects risk positively.
- Ensure only secured wireless network is used.

Security solutions

- Tighten the security measures on use of mobile devices.
- Use email security solutions that help filter and examine the contents of emails.
- Consider using surveillance technology to detect fraud and serious misconduct. This should only be used after conducting the privacy impact assessment.

IPT INSIGHTS

The Australian Prudential Regulation Authority (APRA) information paper on outsourcing involving shared computing services

In July APRA released an information paper detailing its views on prudential risks and issues relating to arrangements involving "shared computing services", including (importantly for many APRA-regulated entities) cloud arrangements. APRA released the information paper because of the "increase in the volume, materiality and complexity of outsourcing arrangements involving shared computing services" raised with APRA as part of the consultation and notification requirements under CPS 231 and SPS 231 (which applies to registrable superannuation entities). The information paper distinguishes between (a) arrangements which involve the sharing of IT assets (including hardware, software and/or data storage) with other parties and (b) 'private cloud' arrangements.

Depending on the response of APRA-regulated entities to the paper, it is unlikely that in the short term APRA will produce a prudential standard that applies specifically to shared computing services, including cloud services. These types of technologies and service delivery avenues continue to develop and evolve. As a result, it would not surprise if APRA and other similar regulators around the world are reticent to produce rigid and prescriptive requirements that could be obsolescent on release. However, if entities take no heed of APRA's observations and suggested practice recommendations, APRA might look to impose an increased level of prescriptive regulation coupled with greater oversight and enforcement.

To find out more contact Nicholas Boyle.

Cloud computing in Hong Kong

The Hong Kong Privacy Commissioner for Personal Data (PCPD) recently published an information leaflet outlining the application of the Personal Data (Privacy) Ordinance (the PDPO) for data users looking to engage cloud providers. The information leaflet outlines the data protection principles (DPPs) which apply in the context of cloud services, and highlights the particular characteristics of cloud computing that give rise to risks from a privacy perspective.

While there are obvious benefits in engaging a cloud service provider, it can also present a loss of control over the processing and storage of personal data rendering it 'higher risk' from a privacy perspective. This does not mean that cloud services should not be used, but it does mean that appropriate steps should be taken to address these risks. Click here for further information.

Cyber risk: What does the future hold?

Cyber insurance is one of the hottest topics in insurance right now, affecting small businesses and governments alike. Jacques Jacobs and Peter Jones, both partners at law firm DLA Piper Australia, tell us how the latest legal developments will affect the space going forward.

Watch now

INTA Meets in San Diego

More than 9,800 trademark practitioners from around the globe convened in San Diego in May for the largest ever International Trademark Association Annual Meeting. DLA Piper celebrated INTA with a series of client events, trademark practice-related discussions and CLE seminars. Nearly 40 DLA Piper lawyers from offices around the world enjoyed connecting with 100+ clients and friends at an exclusive reception held at the Ultimate Sky Box in the Diamond Tower, featuring spectacular views of San Diego's skyline and harbour. Throughout the week, DLA Piper hosted several substantive events, including a CLE event on the new China trademark laws presented by our China-based partners and a CLE luncheon focused on the fashion and retail sector presented by DLA Piper panellists from the US, Australia, Europe, Asia and the Middle East.

Melinda Upton (Sydney) connects with a guest at the VIP client reception

John Nading, Naomi Abraham, Ryan Compton (all Washington, DC), Jennifer Zador (Chief Counsel Licensing, SolarWinds), Ann Ford and Tom Zutic (both Washington, DC)

DLA Piper women trademark lawyers from around the globe gather for a luncheon in San Diego

Clients and partners network at the VIP client reception at the Ultimate Sky Box

MEET GAVAN MACKENZIE

Gavan Mackenzie
Senior Associate
T +61 2 6201 8741
gavan.mackenzie@dlapiper.com

Gavan, you joined the firm in 2006 as a summer clerk, and have risen through the ranks to a Senior Associate. Can you tell us a little about your practice?

I did! I joined the firm back when it was still Phillips Fox. As part of my graduate year, I rotated through the administrative law and government commercial teams. I eventually settled in the government commercial team (which became IPT).

My major areas of practice are information, technology and communication contracts and government procurement. I mostly advise on complex, high value and high profile ICT and outsourcing projects for the Australian government. My clients include the Department of Finance, the Department of Defence and the Department of Immigration.

If you stumbled into my office on any given day, you might find me advising a client on effective procurement methodologies, drafting complex commercial documents, drafting approach to market documentation, evaluating tenders, providing negotiation support or advising on contract management issues.

You have focused your career on Intellectual Property and Technology (IPT), what excites you about the IPT environment?

I've been fortunate to be involved in some of the biggest and most interesting outsourcing arrangements undertaken by the Australian government on a wide range of subjects. I've worked on matters relating to: supporting the Royal Australian Navy's largest ships; establishing whole-of-government panels for ICT goods and services; providing refugee settlement services; preparing blood distribution agreements; outsourcing superannuation administration; and rolling-out of digital television across Australia. It's the variety of subject matter and the nationally significant nature of many of the matters that I work on that I find so interesting.

After spending six months seconded to DLA Piper's UK office, what were the highlights of this experience?

I really enjoyed the chance to work in the UK for six months. It was a fantastic learning opportunity and a chance to work on a significant project for the UK government (led by Andrew Dyson and Richard Bonnar). I worked with a large team across multiple practice groups and offices and it was a real highlight getting to know them all and the work they do – they are all very talented people! It was good to see that, even on the other side of the world, the culture of the firm is largely the same.

Other highlights include the DLA Piper Christmas Party held at the Tower of London, surviving the crushing peak hour on the Tube, walking past St Paul's Cathedral everyday on the way to work, finding the best beer in London (at the Camden Town Brewery) and being able to explore the nooks and crannies of London (and not get lost).

Finally, and on a personal note, can you tell us about your interests outside of work?

I'm a very keen field hockey player. You'll find me at the National Hockey Centre far too often. When I'm not playing hockey, I like to ski, travel and be at the beach. I also spend a lot of time cooking for and entertaining my friends. I also try to improve my photography skills when I can.

Although I haven't been in any shows recently, I enjoy participating in local amateur theatre and love going to see a show. I lost count of how many shows I saw during my short time in London. Needless to say, I absolutely loved being able to pop down to the West End on a regular basis!

WHAT'S ON

Technology and Sourcing Webinar Series 2015

- Government IT Contracting Trends – Tuesday 3 November 2015, 10.00am – 11.00am GMT (Tuesday 3 November 2015, 9.00pm – 10.00pm AEDT)

Practical Legal Training Centre – Sydney – Thursday 12 November 2015

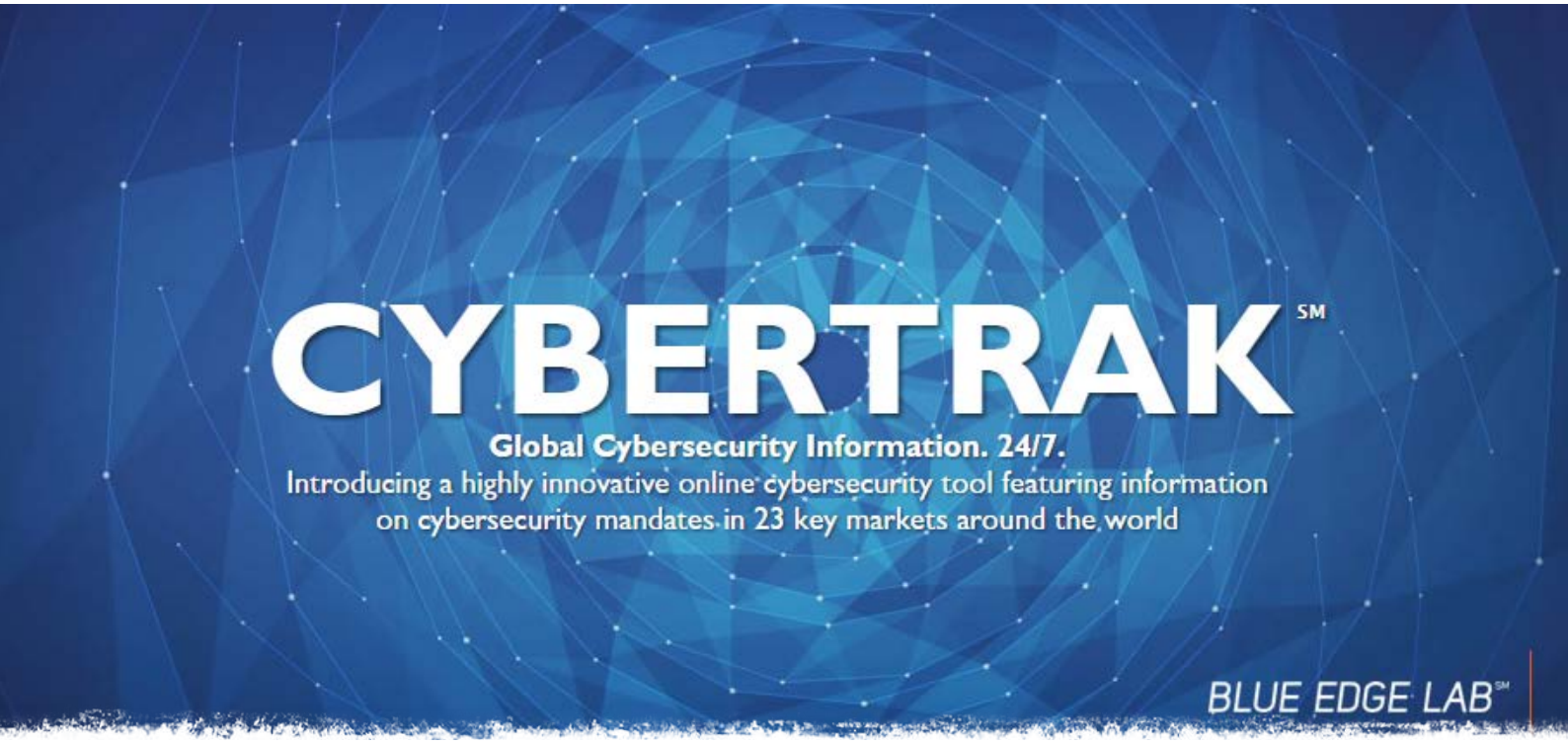
Advancing Your Career in the Public Service – Brisbane – Thursday 12 November 2015

WIN In-House Counsel Day – Canberra – Tuesday 17 November 2015

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.

For further information about our events, or to register to attend an event, please email Events.Australia@dlapiper.com



CYBER COMPLIANCE COUNTS

Because risk associated with a breach escalates quickly in a global marketplace, you need to keep up with the fast-changing laws and regulations in all markets where you operate to ensure you are in compliance. Yet keeping up with dynamic requirements around the globe can be costly and time consuming for multinational companies, diverting valuable time and resources from cyberdefense.

Introducing CyberTrak℠ – the innovative online cybersecurity tool featuring information on cybersecurity mandates in 23 key markets around the world. Sign up for a free trial at www.blueedgelab.com.

CYBERTRAK℠ BLUE EDGE LAB℠