2018 ITechLaw Asia-Pacific Conference
Hong Kong | 8 – 9 March 2018
Written by Jensen Law, Intellectual Property Student, Mayer Brown JSM

Conference Summary

The topics discussed at this lively conference informed the global practice in the intersecting areas of technology and the law. Speakers offered numerous forward-thinking perspectives on areas such as artificial intelligence, FinTech, e-health and cyber security. Legal and social implications of the inception of technology in these areas were explored in detail.

Technology pervades our everyday lives; its undeniable importance and significance attached to us are debated by the speakers of this conference as there involve some common issues relating to data privacy and security. The feasibility of various legal mechanisms, for example an injunction, to solve problems have been evaluated.

Of all the highlighted points, there was one recurring theme: different governmental attitudes, cultures as well as mind-sets between age groups attract different solutions to resolve tensions between technology, governance, and the law. Progression of any of these interrelated variants will always have an impact on the other. Therefore, any correct approach in managing the relationship between technology and society would depend on the interplay between technology, product, legislative climate, culture, existing governing laws etc. To consolidate all views being put forward in this 2-day conference, the one settled premise is that the use of technology should be governed, but the course of such often involves multiple and cross-border issues and always calls for greater attention. As a result, legal advice ought to reflect flexibility yet suitability.

Just as technology brought numerous social benefits, it remains to be seen on how businesses, lawyers and regulators adapt to the ever-growing amount of challenges brought by technology. Through history, we see limitations on what technology can achieve. Nevertheless, its unlimited potentials instigated heated conversations during the course of the conference.

Keynote: The Future of Technology in Asia

Tim Steinert, General Counsel, Alibaba

Mr. Tim Steinert started off his keynote speech with a brief history of Alibaba. He pointed out that they have had tremendous developments in the past years and evolved from only providing business-to-business service to providing business-to-consumer service and from operating a simple listing site to operating multiple transactional sites. At peak, there were 250,000 transactions per second globally that occurred on Alibaba's platforms.

Their technology-driven vision has always underpinned solutions to meet customers' needs. Mr. Steinert stated that for e-commerce to be successful in China, infrastructure and logistic experience of the payment system as well as gaining trust from customers were key considerations. This motivated Alibaba to introduce Alipay. Online platforms such as Taobao and Tmall are also notable services that Alibaba provides. In the earlier days of the decade, the company launched its first e-commerce application on mobile devices.

As a data-driven business, it is important for Alibaba to be at the forefront of all technological advancement. Acquisition of other companies has enhanced Alibaba's ability to meet more consumers' needs and set new directions. Additionally, attention should be given to hardware's intersection with software to support more sophisticated products and services.

Mr. Steinert then acknowledged the demands in how legal services grow not just in volume but also for expertise in certain areas. Developments in the technology field advance at the speed of light and lawyers need to renew their technological knowledge to be more productive in providing legal services. Dynamics in the field and internationalisation have also been shaping the size of the Alibaba legal team. Just as technology drives efficiency in the operation of legal services, some common issues faced by multinational businesses like Alibaba include the conflict of different regulatory requirements around the world, data privacy, data security, labour, patent, export of licence, correct allocation of resources etc.

To close the keynote speech, Mr. Steinert stated that technology is changing all our lives and we must keep up with the demands and up our game in order to provide more valuable services to customers. It is exciting to have new technologies being provided to the world, but at the same time we need to be cautious about the legal implications that they bring to us. It is noted that the world, as an interactive space, is going to be "*tougher and tougher*".

How Intelligent Are We?

Moderated by Charles Morgan, McCarthy Tétrault LLP
Neil Sternthal, Thomson Reuters
Dan Hunter, Swinburne Law School
Jake Lucchi, Google

(i) The potential of AI to the legal profession

The panel first explored the transitions of AI technology and the reasons it prospered. The speakers provided an overall view that the current achievements were products of great collaborations amongst architects and would not have been anticipated 10 years ago. It is the decrease in the cost of computing power, an increase in the availability of data and the wider range of applicability of machine learning to different fields that caused AI to become more common.

Charles Morgan then quoted an article by Google which referenced an analogy comparing AI to a 4-year-old child and how much time is required for said child to become a full adult. Jake disagreed with this analogy and commented that the operation of AI technology is largely based on human's instructions. It would be a better analogy to describe AI as an adult with narrow interest.

The effectiveness of an AI's output depends on the quality and structure of the datasets that were given to an AI. Practices such as trademark registration, probate, divorce and other areas which have a lower level of consumer base, involve simpler type of transaction or legal research could be benefited most from the utilisation of AI. It is well-known that AI outperformed human in efficiency tests. Also, big data is what it takes to produce meaningful results by AI and it is inevitable that AI would get "*smarter and smarter over time.*"

(ii) The risk of AI in relation to the legal profession

In times of big data, there lies the challenge of ensuring privacy is protected because a broad range of data could be used by AI. Datasets are crucial to the functioning and success of AI. "*Competition is very robust*" in the technology field and data credibility could be a differentiating factor that companies would rely on. However, smaller companies would be in disadvantage as they are less likely to have access to extensive datasets than larger companies. Furthermore, it is acknowledged that bias exists in the decisions made or results produced by AI. The speakers rebutted the statement by stating that flaws such as race discrimination also exist in human decisions. The biggest challenge to this is the difficulty in identifying the reason why biased results were generated by AI. Additionally, grey areas such as who bears the liability in the event of AI dysfunction and ownership of work produced by AI remain unsolved.

(iii) The regulation of AI and its impact on the legal profession

The panel agreed that a legal framework is important to govern AI. Considerations such as knowing the specific risks and implications of utilising AI in a certain industry, and the overall legislative climate within a continent would paint a better picture of what regulatory models are best.

Going Digital

Moderated by Chris Perera, AT&T, Asia Pacific
Stephen Mathias, Kochhar & Co.
Fiona Phillips, HSBC
Kelly McFadzien, Chapman Tripp
Pindar Wong, VeriFi (Hong Kong) Ltd.

At the beginning of the discussion, all speakers acknowledged technology's role in bringing the world forward and fundamentally changing the mode of interaction between humans. It is noted by Pindar Wong that "*we have the flexibility of change, but we also have the responsibilities on the system that we are designing*". In terms of governance, simplicity of a legal framework and smooth operation are key to success. This calls for contributions and collaborations amongst lawyers, judges and engineers. In addition, it is crucial for the government to understand the nature and implications of disruptive technologies to the society, and to identify the various needs or trends that ought to be addressed. For example, the attitudes towards data privacy vary not only across countries but age groups; younger people are more used to the digital environment and are less demanding in protecting their privacy.

The panel then moved on to discuss the nature and scope of privacy law. Fundamentally, the challenges for addressing cross-cutting issues are the rate of change in this digital age, as well as the difficulty in prioritising which problems to solve first. The traditional consent model of privacy law was explored by the speakers and they also discussed whether principle-based regulations, such as the GDPR, would succeed. Just as the law should adapt to trends or changes, the idea of using legal mechanism to protect privacy was questioned because "*what's the point of being private in a non-private world?*"

The speakers were asked for their opinions on whether the law is going to bend according to technology, or vice versa. The speakers opined that it is possible to have a mixture of both scenarios. To provide another perspective, Fiona Phillips suggested that even we can only innovate within the constraint of the law, sometimes we are the barrier to progress as laws are created by humans. Kelly McFadzien proposed that we should focus on deliberating the practical elements of the system such as the appropriate types and regulatory level of the laws.

The risks that AI could bring to humanity were re-explored towards the end of this session. In particular, the concern in relation to AI's tendency to outperform humans in certain aspects was discussed. Pindar countered the concern by suggesting anthropology could answer people's growing distress over AI's potential takeover, because he foresees all future jobs are empathetic jobs, which are irreplaceable by emotionless machines.

The Anatomy of a Cyber Attack

Moderated by Anna Gamvros, Norton Rose Fulbright
Stephen Kai-yi Wong, Privacy Commissioner for Personal Data of Hong Kong
Elaine Lim, AIG Insurance Hong Kong Ltd.
Laura Tyson, FleishmanHillard
Brian Wilson, KPMG

The anatomy of a cyber attack was discussed in the context of regulations, forensics, public relation and insurance. Stephen Wong, the Privacy Commissioner for Personal Data of Hong Kong, explained that the local regulatory regime is in constant review, so as to ensure its applicability to the current technical advancement. In particular, the laws being technological neutral is one of the main features of HK data privacy law. A few examples of real data breaches in Hong Kong were raised and a comparison between the Personal Data (Privacy) Ordinance and the GDPR was made. The three elements that stakeholders should be aware of in relation to data breach are – *protection*, *responce* and *recovery*. A company could be protected from data breach by having adequate audit, complying with the governing laws and regulations, and preparing emergency protocols. A structured breach response plan should also be prepared for swift response in the event of data breach. It is crucial to engage with professional experts to support recovery of a data breach.

From the perspective of forensics, Brian Wilson also agreed preparation is key but often absent from many corporations' operations. Educating employees and having a sustainable programme that monitors data flow are examples of adequate schemes. He also noted that different regions have different views in respect of data breach. For example, data breach in America is an event that happens "*like every other day*"; and that in Asia, "*privacy is a big thing, and people really care about it*".

A company might encounter huge reputational risks in an event of data breach. It is essential to communicate at the very first available opportunity, prepare statements in advance and also make available up-to-date internal policies and training details. Also, it was emphasised that a cyber insurance will not prevent a cybercrime, but only ensure a company would be in a financial footing when an incident occurred.

A scenario of a "spear phishing" scam was presented to the panel and the speakers were asked to explain proper reactions to such case. In general, the speakers re-emphasised the above points and approaches, and further highlighted the importance in having and allocating correct resources for the sake of damage control.

FinTech and RegTech – Navigating the Latest Trends and Challenges

Moderated by András Gurovits, Niederer Kraft & Frey Ltd.
Jonathan Fairtlough, Kroll Associates, Inc.
Oliver Yaros, Mayer Brown International LLP
Nick Beckett, CMS Beijing
Michael Wong, IBM Global Business Services

At the outset, András Gurovits posed the common question of whether FinTech is in a position to replacing banks to the panel. The following discussions suggested that not only FinTech did not replace banks, there has been a wider integration of technology and financial practices now, but also growing difficulties in tackling online financial crimes.

FinTech is an innovation that influenced the retail and institutional spaces. It has been a significant move to modernise financing. Notwithstanding, the misuse of technology for criminal means in this context suggests a departure from the traditional concept of physical appropriation to online theft. It is also common to involve multiple parties to the process of operating FinTech and this is the exact point of failure of the current prevalent finance system. Also, the platforms for cryptocurrency are potent environments for financial crime. Resultant issues include the identification of targets and effective law enforcement in the online world. In other words, the underlying technical and transparency issues prevail. Laws are built based on territorial construct and solutions now need to address a system which was designed to specifically defeat such construct.

Prevalent uses of FinTech can easily be evidenced in China, such as the use of WeChat Pay or Alipay. FinTech is often used in payment, process efficiencies, insurance, deposit, lending, investment management and fundraising. In China, many vendors are even refusing to accept cash and such illustrated the interactions or the mode of transactions have been profoundly changed due to FinTech. Attention needs to be paid to this social or business trend. Nick Beckett then identified the reasons that propelled the rapid growth of FinTech in China, including the commissioning of innovative initiatives, large consumer base, high availability of capital enthusiasm in new business and a large pool of technical and entrepreneurial talents in China. Legal issues that stemmed from these are relating to data protection, and the balance between innovation protection and the spread of new technologies.

In addition to the aforementioned legal issues, Oliver Yaros also pointed out that other typical issues include the viability and sophistication of the FinTech businesses, the inability to understand the suitability and limitations of the underlying technology, and the governance of data used by FinTech.

Towards the end of this session, there were further explanations on the benefits that blockchain could brought to the commercial world and the utilisation of AI in an early warning system for the purpose of identifying alarming behaviour.

Content is King?

Moderated by Julian Potter, WP Thompson
John Medeiros, Cable, Satellite and Broadcasting Association Asia (CASBAA)
Peter Ruby, Goodmans LLP
Rahul Matthan, Trilegal

The prevalence of fake news and content piracy suggest that we should pay attention to both the content and other aspects of content delivery. In regard to fake news, Rahul Matthan noted that the Internet has enabled easy dissemination of information in a cross-border manner, implying the difficulty in fighting against the spread of fake news. Nevertheless, Julian Potter pointed out that human behaviour is the ultimate cause of the spread of fake news and that technology is just an enabler. Instead of putting forward conflicting facts to correct the incorrect views of readers, it would be much more efficient to challenge their underlying beliefs that drove them to believe the false news in the first place.

In view of the current golden age of television, content and online piracy posed great threats to the TV and broadcasting industry. The online distribution of content usually involves operations in multiple jurisdictions, and that governing laws regarding piracy could differ across countries. This situation paved ways for infringement syndicates to avoid responsibilities by hiding in non-cooperative jurisdictions. Lessons from the past indicated the ineffectiveness of using international treaties to address the problems. Proactive mentality of the law enforcement and having an up-to-date copyright regime are possible way outs. Furthermore, Peter Ruby explained the ineffectiveness in using conventional court injunction to stop illicit online activities, and cited an example of the tension between a Canadian court and an American court – that the courts adopted different attitudes towards granting or enforcing an injunction in relation to a cross-border matter. It is the latter court that emphasised the importance of balancing the freedom of speech and privacy right; thus the injunction was declared unenforceable. This illustrated that even "*the content was king, it was the context that drove the result*" in a post-territorial world.

From a commercial perspective, monetary value is attached to the content and the technical aspects of content delivery have become more important. For instance, immediacy and timeliness of delivery of a live football match are crucial to the audience. Citing Netflix as an example, the quality of videos, search engines and content recommendation are other considerations that determine the success of a business. The use of AI in supporting these kinds of client expectations would not be surprising. Diversity of the content and distribution methods are also dependent on a business' client base. The tremendous amount of users' information collected as a result has underlined a "big data issue", which reverts back to the question of appropriate governance of AI, rather than the content. As it is the monetary value attached to the content that motivates businesses, perhaps, as Julian Potter suggested, "*cash is king*".

All You Ever Wanted to Know About China but were Too Afraid to Ask

Moderated by Michelle Chan, Bird & Bird
Elaine Ann, Kaizor Innovation
Dennis Cai, Internet Dot Trademark Organisation Ltd.
Sheng Huang, Covington & Burling LLP

This panel reviewed the means of protecting information, IP and technology in China. The underlying principles and culture that shaped the Chinese regulatory environment today were also discussed. Patent applications have been growing in volume and most were applied by Chinese companies. An alternative way to assert rights in China in this context include a reliance on the doctrine of trade secret. Yet, the best form of protection to clients' interest depends on the length of protection that best suits clients' needs.

China, being a highly populated country, offers bigger business opportunities than other countries. As such, Elaine Ann suggested a notion of "*China math*", which means the consideration that a business may take into account when deciding the price per unit of its products. Given China has a huge consumer base, selling a product at a lower price may suffice to attract greater return or revenue.

Global brands and the so-called "Chinese versions" both exist in China. The speakers identified the issues of counterfeiting goods being sold online and the use of confusingly similar domain names by infringers to lead Internet users to fake online business platforms. Litigation through specialist courts in China could be a possible solution. However, to tackle problems of this kind requires utilisation of technology and adherence to certain procedures. It was pointed out that infringers are always at east to set up another domain name online. Despite this, many Fortune 500 companies have chosen Chinese courts as venue for dispute resolution. This is a fact that countered common biases against Chinese courts being incompetent in handling matters of technical nature. Whilst injunction is a common relief that the parties are seeking, Sheng made comparisons between the different rules for granting injunctions in different jurisdictions. It was highlighted that there were indeed more foreign companies lodging IP claims in China than local ones. Other dispute resolutions such as arbitration were also evaluated by the panel, and the issue of recognising a foreign arbitral award could be a problem in certain jurisdictions. The possibilities in protecting information as trade secret or through non-compete agreements were also explored. It was suggested that a contractual claim might be easier to succeed than a case on trade secrets in China.

The audience was concerned about the confidentiality and security of online information, especially those stored in cloud services, due to the prevailing common suspicion of the Chinese government having the encryption key(s). According to the speakers, it is the history and culture of China that propelled the Chinese government to do whatever it takes to achieve harmonisation within the country, including the means of seeking control over information. Just as the Chinese government may not stop monitoring, the process of conducting could become more transparent in the future.

Developments in E-Health and Health Technology

Moderated by Claire Bernier, ADSTO
Jonathan Sternberg
Peter Huppertz, Hoffmann, Liebs Fritsch & Partner
Sheena Jacob, JurisAsia LLC

In this session regarding e-health, the speakers introduced the current practice of healthcare service in this digital age and the challenges brought by the relating innovations. Jonathan Sternberg foresaw that new, efficient and emerging business models would challenge existing healthcare institutions and bring clinical impacts to the services that they provide. Digitalisation, big data and AI would alter the healthcare sector. Even so, the aims of e-health technology include offering a borderless healthcare ecosystem for enhancing accessibility to quality healthcare and the efficient use of medical resources. However, issues that ought to be addressed include the regulation of the storage, usage and privacy of data, the management of cost sustainability due to the high R&D cost in both the technology and healthcare sectors.

Peter Huppertz provided insights into the GDPR and identified the problems arising out of its vague and undefined terms. In addition, Sheena Jacob gave an overview of some on-going initiatives in Singapore, which aim to drive efficient operations of healthcare services. However, 'e-health risks' exist and typical issues such as cyber security, privacy and data protection, ownership of liability and jurisdictional problems continue to pose risks.

The outreach of the GDPR was questioned again and the speakers were of the view that there remains unresolved grey areas. The audience was surprised by this answer as Article 3 of the GDPR has already provided clear answer to its territorial scope. Discussions on the necessity of having privacy impact assessments within institutions, the differences between the technical and legal definitions of anonymisation were conducted towards the end of this session.

Startups: In Search of the Unicorns

Moderated by Philip Catania, Corrs Chambers Westgarth
Gladys Chun, Lazada Group
Siddharth Rao, Sequoia Capital India
Julius Wang, Reylabs
Knut Fournier, Gobee.bike

There are numerous matters, such as the legal, business and financial implications of a decision that start-ups need to be aware of. Deducing from her experience in Lazada, Gladys Chun explained the bedrock and crucial parts of start-ups – their structures, finance and branding. The due diligence involved and acknowledgement of shareholders' values remain essential. Siddharth Rao concurred and suggested that the embrace of the right governing jurisdiction in a contract or agreement is another significant factor worth considering, as the current trend is moving towards an online borderless platform for businesses. Given the limited financial resources that start-ups have, prioritising the funding of various needs is of the essence. Developing good relationships with service providers is another key.

It is not doubted that a successful business model could be premised on the amount of funding a start-up has, and such could be dependent on the quality of legal advice that the start-up receive. However, quality legal services are not cheap. The power of network was highlighted by the speakers, and seeking inform legal advice could be an interim solution to start-ups. The panel also suggested the idea of having a data room containing information ready for potential investors upon request.

The opinion of the floor was that current start-ups focused too much on offering new ideas to the market, and zealously conducting patent searches to identify new business opportunities. Whilst the attempt in differentiating themselves from competitors is not a bad idea, start-ups need to understand the motivation for other businesses to exploit the patent system could be for strategic reasons only. Furthermore, regulatory awareness is important because it is common to have a mismatch between what the law expects and how people interpret it. Politics in each country could also determine a start-up's success.