CAMLA COMMUNICATIONS LAW BULLETIN

Communications & Media Law Association Incorporated

Volume 34, No 4. January 2016

Copyright in a Meme

Ryan Grant considers what copyright exists in a 'meme' and whether its author has any protection under Australian copyright laws.

Several press articles have made the somewhat obvious assertion that a meme will usually infringe a third party's copyright in the underlying image, unless there is a fair dealing defence.[1] However, little consideration has been given to whether the meme itself is provided with copyright protection. In this article, I look at whether the creator of the meme (a ***Meme Author***) can enforce copyright in an image meme, even if the meme infringes a third party's rights in the underlying image.

WHAT IS A MEME?

A meme, or more correctly in this context, an image meme, is typically an image distributed on social media where some short text is placed over a pre-existing image. The combination of the text with the image, or more importantly, the subject relationship between the text and image is used to make a joke or political statement.

Often, the Meme Author will not have a licence to use the underlying image. Other times, the Meme Author will have a licence because the Meme Author is the author of the image or the image is subject to a broad type of licence, such as some types of creative commons licences.

Memes have evolved from social media jokes to useful marketing tools. Greenpeace, Dos Equis and Blizzard have all used image memes to promote their causes or products. Further, a business that has a social media presence may well encounter its customers posting memes on their social media pages, possibly without permission of the Meme Author.

SUBSISTENCE OF COPYRIGHT

Type of work

The *Copyright Act 1968* (Cth) grants copyright in original literary, dramatic, musical or artistic works[2].

The term 'artistic work' is defined (exhaustively) as:

(a) a painting, sculpture, drawing, engraving or photograph, whether the work is of artistic quality or not;

(b) a building or a model of a building, whether the building or model is of artistic quality or not; or

>

1 http://www.news.com.au/technology/online/why-creating-memes-is-illegal-in-australia/story-fnjwmwrh-1226758121774 and http://www.insidecounsel.com/2013/06/21/technology-internet-memes-pose-legal-questions.

2 Section 31 Copyright Act 1968.

CONTENTS

Copyright in a Meme [CONT'D]

> (c) a work of artistic craftsmanship whether or not mentioned in paragraph (a) or (b).

The term 'literary work' is defined[3] to include (non exhaustively) *'a table, or compilation, expressed in words, figures or symbols'*. The term 'compilation' is not defined in the Act but has been the subject of judicial consideration.

an image meme, being the combination of an image and some text, and perhaps some other diagrammatical features is very likely to be a 'literary work' under the Copyright Act

The courts have found that an edition of a newspaper is a single compilation work, including the articles, heading and layouts.[4] Further, a set of hard copy accounting forms (it was 1985) created to assist in the production of accounts for businesses was found by the Queensland Supreme Court to be a copyright work.[5] Comments from Thomas J in that case (at 231 and 232) are instructive in these circumstances:

> The columns, boxes and lines are in my view, drawings, and as such comprise an "artistic work" within the definition of that term. It follows that every document in issue in this case comprises in part a drawing which is capable of being an artistic work, and in part words which are allegedly capable of being a literary work. It is not necessary that components of a compilation be explicitly literary . . . For present purposes, it is enough to say that a compilation of forms which are themselves an integrated combination of words and drawings is a compilation for the purposes of the Copyright Act, and as such is within the definition of "literary work" under that Act... In my view there is no requirement that a compilation be of component works that are exclusively literary.

The Kalamazoo case has been followed by a number of courts, including a Full Federal Court decision involving a computer program that produced Material Safety Data Sheets (MSDS).[6] An MSDS contains a series of text fields, diagrams, images and symbols that detail statutory information that must be supplied with certain products. The first instance judge and the appeal Court had little trouble finding that the combination of the various elements meant that the MSDS was a 'literary work; under the Copyright Act.

Accordingly, an image meme, being the combination of an image and some text, and perhaps some other diagrammatical features is very likely to be a 'literary work' under the Copyright Act.

The next question is whether an image meme can be sufficiently original to attract copyright protection, particularly in circumstances where the Meme Author does not have a licence to use the underlying image.

ORIGINALITY

For a work to gain copyright protection, it must be an original work created by an author. Originality will require the examination of two, closely linked, issues. The first is whether the meme is just a copy of other material and the second is whether sufficient 'independent intellectual effort' and/or 'sufficient effort of a literary nature' has been exercised by the author.

An oft-cited case on originality is *Victoria Park Racing v Taylor*[7] which said at 511:

> No doubt the expression literary work" includes compilation. The definition section says so (sec. 35 (1)). But some original result must be produced. This does not mean that new or inventive ideas must be contributed. The work need show no literary or other skill or judgment. But it must originate with the author and be more than a copy of other material.

There was some debate in Australian law as to whether labour alone was sufficient to give rise to copyright. However, in the case of *IceTV v Nine*[8] the High Court stated at [33] that labour alone was not sufficient:

> Originality for this purpose requires that the literary work in question originated with the author and that it was not merely copied from another work. It is the author or joint authors who bring into existence the work protected by the Act. In that context, originality means that the creation (that is the production) of the work required some independent intellectual effort, but neither literary merit nor novelty or inventiveness as required in patent law.

Even if the Meme Author does not own copyright in the underlying image, the positioning of original text over a particular image to make a political statement or joke will usually to give rise to a copyright work. It is clear that it is not just a copy of the underlying image. It is the combination or subject relationship between

3 Section 10 Copyright Act 1968.
4 *Fairfax v Reed* (2010) 189 FCR 109.
5 *Kalamazoo (Aust) Pty Ltd v Compact Business Systems Pty Ltd* (1985) 5 IPR 213.
6 *Acohs v Ucorp* [2012] FCAFC 16.
7 *Victoria Park Racing and Recreation Grounds Co Ltd v Taylor* (1937) 58 CLR 479.
8 *IceTV Pty Limited v Nine Network Australia Pty Limited* [2009] HCA 14.

the original text and the image that requires the intellectual effort.

It is possible that, if the text is not original to the Meme Author and the image is not owned by the Meme Author, meaning the Meme Author simply brought the two items together, that the work is not sufficiently original, in that not sufficient independent intellectual effort has been brought to bear. However, given the low threshold for originality, such a situation would be in the vast minority.

PROTECTION OF A COMPILATION THAT INCLUDES INFRINGING MATERIAL

While covered to some extent above, I also specifically address below the question of whether a work that infringes another person's work can itself be the subject of copyright protection. A number of cases in Australia and the UK have found that compilations of entirely pirated works can attract their own copyright protection (including *Redwood Music Ltd v Chappell & Co Ltd* [1982] RPC 109). Drummond J in *A One Accessory Imports v Off Road Imports* (1996) 34 IPR 306 at 317 said:

Skill, judgment or labour expended in the process of copying a particular work or portion of a particular work, as distinct from selecting material to be copied into a compilation, cannot confer originality; but even if the effort involved in producing a compilation is mostly devoted to copying another work or works, a relatively small alteration or addition quantitatively may suffice to convert that which is copied from an earlier work into a new and original work in which copyright will subsist. Whether it does or not is a question of degree having regard to the quality, rather than the quantity of the addition.

Accordingly, very little additional intellectual effort needs to be put into the work over and above the potentially infringing underlying image for a meme to attract copyright protection.

INFRINGEMENT

The Meme Author as the owner of the copyright in the meme has the exclusive right, relevantly to online use, to make a reproduction or communicate the work to the public (including making it available online). If another user (***Defendant***) copies the entire meme and makes it available online, that user is likely infringing the Meme Author's copyright.

Obviously, if the Defendant only copies the underlying image, the Meme Author does not have an action against the Defendant as the Meme Author does not hold the copyright in the underlying image.

On proceedings for infringement, the fact that the work at suit is itself infringing another person's copyright can give rise to public policy considerations as to whether the Meme Author is entitled to relief, despite being able to prove infringement.[9] However '*the mere existence of an infringement of the copyright of a third party (especially an innocent, rather than deliberate infringement) was not sufficient to invoke this jurisdiction*.[10]

In the ZYX case from the United Kingdom, the facts showed that ZYX did not know that the work it had been assigned (a song) infringed a third party's copyright. Accordingly, the United Kingdom High Court found that ZYX was entitled to the relief sought, including damages and an injunction.

Conversely, in the separate judgment on relief arising out of the *A One Accessory case*[11] , the Australian Federal Court found that, while the respondent had infringed A One's copyright in a parts catalogue, because the parts catalogue at suit was in large proportion copied from a third party by A One, the Court refused to grant any equitable relief to A One because A One had '*unclean hands*'. Drummond J said at 562:

Adopting the approach in Moody v Cox and Hatt [1917] 2 Ch 71 at 87–8, I think that the dirt on the applicants' hands, constituted by their extensive copying of the works of others, is so closely related to the equity claimed in the form of an injunction to restrain Off Road's use of its own infringing catalogue as to justify denying the applicants relief under s 115(2) of the Copyright Act 1968 (Cth).

very little additional intellectual effort needs to be put into the work over and above the potentially infringing underlying image for a meme to attract copyright protection

As a result, A One was refused an injunction or declaration, leaving A One with a damages claim only.

Accordingly, a Meme Author will likely be successful against a person who posts the meme online, even if the underlying image infringes a third party copyright. However, depending on the particular qualities of the meme, including whether the author knew it was infringing and the inherent creativeness of the final meme, it is possible that the Meme Owner will not be able to seek injunctive or declaratory relief.

RYAN GRANT is a Senior Associate in the Media and Content Group at Baker & McKenzie in Sydney.

9 *ZYX Music GMBH v King* (1995) 31 IPR 207; *Venus Adult Shops Pty Ltd v Fraserside Holdings Ltd* (2006) 238 ALR 534.
10 *ZYX Music GMBH v King* (1995) 31 IPR 207 at 215.
11 *A One Accessory Imports v Off Road Imports* (1996) 144 ALR 559

Internet of Things – Is it Hype or the Next Big Thing? Part II

James Halliday and Rebekah Lam provide the second and final instalment in a two-part series which examines the legal and policy implications of the Internet of Things (IoT).

The IoT reflects the maturity or industrialisation of the internet and is being enabled by rapid improvements in sensor technology, bandwidth and mobile technology generally and big data analytics. The IoT therefore creates unprecedented opportunities as well as risks. In Part I which appeared in Volume 3 of the 2015 CAMLA Bulletin we looked at some of the issues arising for industry including interoperability and standards; numbering plan and roaming implications; and spectrum allocation policy and net neutrality issues.

Having to provide the required notice and obtain the relevant consent at each juncture is in many cases impracticable

We now turn our attention to a range of law enforcement and consumer issues arising out of the IoT in Australia, and in particular what the IoT means in the context of cybersecurity, personal privacy and general consumer law. While a single IoT device in itself is most likely harmless, when aggregated together in the millions these devices pose considerable challenges and potential harm, whether intangible, inadvertent or malicious.

CONSUMER LAW

In (very) general terms, the existing Australian consumer law framework will mostly apply to IoT applications supplied to consumers. This framework prohibits misleading or deceptive conduct, implies statutory guarantees into certain consumer contracts, establishes a product liability regime and may also void unfair or unconscionable contracts. The existing privacy protection framework will also apply where a regulated person (such as an IoT operator) collects, uses or discloses personal information about a consumer. These are valuable protections for consumers.

THE AUSTRALIAN CONSUMER LAW

Consumers who purchase IoT products receive general protection under the Australian Consumer Law (***ACL***). Although not specific to the IoT, the ACL protects consumers from misleading or deceptive conduct, unfair contract terms and unconscionable conduct. The ACL also contains statutory consumer guarantees (e.g. goods must be of acceptable quality, match their description, be fit for purpose) which is a further, albeit n indirect way of enforcing privacy and security compliance.

For example, in the USA, after a man hacked into a baby monitor in 2013, the FTC (the Federal Trade Commission) took its first action against an IoT firm for misleading or deceptive conduct. The FTC alleged that TRENDnet – a web enabled camera manufacturer promised customers that its cameras were secure, when they were not.[1] The claim was settled by the parties and the terms of the settlement required TRENDnet to address the security risks, help customers fix their software and obtain an independent assessment of their security programs every year for 20 years. TRENDnet was also prohibited from misrepresenting the security of its cameras or the security, privacy, confidentiality or integrity of the information that its cameras or other devices transmit and the extent to which a consumer can control the security of information stored, captured, accessed or transmitted by the devices.[2]

In Australia, under the ACL, "consumers", are broadly speaking, persons who acquire goods and services that are priced less than $40,000 or goods or services of a kind ordinarily acquired for personal, domestic or household use or consumption. Equivalent legislation exists at the State and Territory level.

The ACL is administered by the Australian Competition and Consumer Commission (***ACCC***), which (in addition to its general enforcement powers) has special powers under the *Competition and Consumer Act 2010* (Cth) (***CCA***) to promote competition within the Australian telecommunications industry and ensure consumers' interests are protected.

PRIVACY LAW

Australian privacy law regulates the way that personal information (information about an individual who is identified or reasonably identifiable) is collected, used, stored and disclosed. The privacy laws include 13 Australian Privacy Principles (***APPs***) which apply to most government agencies, private organisations with an annual turnover of $3 million or more, health organisations, bodies that trade in personal information and parties that contract with the Commonwealth.

1 Peppet, Scott, Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent, 93 Tex. L. Rev. 85 2014-2015.

2 https://www.ftc.gov/system/files/documents/cases/140207trendnetdo.pdf.

CONSENT REQUIREMENT

The privacy regime imposes a transparency framework for general personal information and a consent requirement for the collection of sensitive information. Under this regime an organisation that collects personal information (***APP Entity***) must notify the data subject about specified matters such as what information is being collected, how it is collected and how it will be used and disclosed.

In theory, a data subject wishing to control the collection and use of his or her information could consult the relevant public disclosures made by each relevant service provider and elect not to deal with a provider that does not propose to use personal information in an acceptable manner. However, this is difficult to achieve in practice since data subjects usually have little scope for negotiating privacy terms and have limited control over the collection and use of their personal information. In certain circumstances, due to the pervasive nature of IoT devices, it is possible for an IoT service provider to collect information about an individual without the individual's knowledge (e.g. facial recognition technology, public wi-fi spaces).

Where personal data is collected with an individual's knowledge, the APPs require IoT service providers to provide details of who owns the data collected by an IoT device, exactly what data a device collects, how the data is protected, who the data is shared with (including any overseas recipients) and the specific purposes for which the data is used. However, in many cases this is impractical or impossible, particularly where there is no transaction with the data subject and therefore no means of directly communicating with them. As there is no tort of privacy in Australian law, a data subject presently only has a legal complaint if they can demonstrate a breach of a duty of confidence, as set out in the Lenah Game Meats decision. This is typically difficult or impossible where the data subject has been subject to 'surveillance' in a public space.

Also, because the IoT industry is evolving a further complexity arises. Quite often, the type of data initially collected by an IoT device is put to different uses over time. Whilst an individual may have consented to the initial uses of the data, the consent will generally only apply to subsequent uses if the secondary use is directly related to the initial use. Having to provide the required notice and obtain the relevant consent at each juncture is in many cases impracticable.

In summary, consent in the context of the IoT may therefore not always be a feasible way of managing privacy expectations. What is perhaps more important is for the individual affected to understand the use to which the data is put and the opportunities, if any, to access and review that data.

AGGREGATION OF DATA

Issues also arise when data sets that do not initially contain personal or sensitive information (and are therefore not regulated) are subsequently aggregated with other data sets and become regulated. For example, information regarding the location of a particular mobile device over time combined with mapping and other public database information could reveal an individual's home address, work address, age, health, faith and many other personal details including name and phone number. This would convert non-personal information to personal information that is subject to privacy law.

This aggregation of data was highlighted in the case brought by Ben Grubb against Telstra when Telstra denied him access to his metadata (e.g. geo-location data). By failing to provide the journalist with this information, the Privacy Commissioner found that Telstra had breached the Privacy Act. In its defence, Telstra had argued that metadata was not personal information about a customer because on its face, the data was anonymous. The Privacy Commissioner rejected that argument on the basis that the cross matching of that geo-location data with different data sets could identify the customer, therefore converting the geo-location data into personal information.

DATA MAINTENANCE

Under APP 11, an APP Entity is required to destroy or de-identify personal information when it no longer needs the information and must, on request, give an individual access to his/her personal information within a reasonable period unless an exception applies e.g. it could be said that the granting of access would reveal commercially sensitive information or compromise the privacy of another person. (APP 12). If an individual's request is denied, the collecting entity must explain the reason for the refusal and the mechanisms available to the individual to complain about the refusal.

consent in the context of the IoT may therefore not always be a feasible way of managing privacy expectations

In the IoT context this requirement could involve thousands of requests from data subjects creating an enormous administrative burden and one which IoT service providers would be ill-equipped to handle. It is also likely to be difficult to provide this data in a way which is meaningful to an individual, as much of the data's value is derived from aggregating it with other information.

Concerns have also been expressed regarding whether some IoT sensor data can truly be de-identified given the unique fingerprints of many devices and the ability to re-identify the data. It may be impossible for data captured by some IoT applications to comply with the de-identification requirement since is it unclear whether these data sets can be truly anonymised.

Another concern is the 'portability' of data. There is no common or required standard for how data is stored and practically it would be difficult to introduce one. However, if an individual changes service providers they will typi-

>

> cally want their data to be ported to the new service provider, which is often difficult or impossible, thereby creating barriers to choice.

CYBERSECURITY

The security of captured data faces increasing risks as the IoT becomes ubiquitous and cybercriminals understand the value of the information. The range and number of devices and disparate networks that are being used expands the number of potential targets for cyber threats.

The security of captured data faces increasing risks as the IoT becomes ubiquitous and cybercriminals understand the value of the information

Low powered special purpose devices typically used for IoT do not have the processing power to maintain high levels of security. The small form factor and low power and computational capacity make adding encryption or other security measures difficult.[3] Network devices that accept connections from limited function internet-enabled devices may also have increased vulnerability.

Malicious attacks are becoming more and more sophisticated, varied and harder to defeat. A study by HP revealed that 70% of the most commonly used IoT devices contained vulnerabilities.[4] The increase in the number of devices can also mean vulnerabilities spread very rapidly.

Adding to this risk is the fact that the risk landscape is pushing well beyond the boundaries of a particular organisation, since organisations are owning less and less of the data assets flowing through their systems. Security measures must encapsulate a much wider network beyond the organisation and address the standards of security of the organisation's clients, customers, suppliers/vendors and business partners.

The FTC recently published guidance on what companies should consider when they design and market products that are connected to the IoT.[5] The recommendations largely contain standard security protocols e.g. encryption, limited permissions, two-factor authentication and regular security evaluations. They also reiterate the need to be much more vigilant given the pervasive nature of the IoT in a workplace and also at home. The guidelines centre on the principles of security, data minimisation, notice and choice. The FTC recognises that businesses and law enforcers both have a shared interest in meeting consumer expectations regarding the security of new IoT products.

The FTC guidelines reflect that IoT products are not always engineered to protect data security as they are often created by consumer goods manufacturers and not computer software or hardware firms. Many IoT products are also not designed to be re-tooled after release to the market so are not patchable or easy to update.[6]

The FTC guidelines recognise that there is no one-size-fits all approach to guarantee the security of connected devices. They also recognise that those companies which take the lead in providing consumers with confidence about how their data will be used, are the most likely to flourish from the IoT revolution.

The FTC, however, concludes that any IoT specific legislation would be premature given that the technology is still emerging and is rapidly changing. However, the FTC is calling for stronger data security and data breach notification legislation to provide some measure of protection to data subjects. It is also asking for manufacturers to engage in privacy by design i.e. building privacy safeguards in their products upfront given that many connected devices have little or no user interface.[7]

As a reflection of its commitment to harnessing the value of the IoT, the US Senate passed a resolution in March 2015 calling for a "national strategy for the IoT to promote economic growth and consumer empowerment".[8] The resolution referred to the US prioritising the development and deployment of the IoT in a way that "responsibly protects against misuse" but did not go further to mention anything about how the IoT would be regulated.

PRODUCT LIABILITY

In addition to the risk of an IoT product malfunctioning and causing damage to property or physical injury, IoT devices are vulnerable to cyberattacks which may cause damage or injury (e.g. a compromised heating system could cause fire and property damage). Liability may also arise to an IoT user if their personal data is used by a hacker in an attack on a third party or to breach that third party's privacy rights.

In situations where an IoT product causes loss, identifying who bears responsibility if the software is vulnerable to cyberattack and what role the consumer plays are not necessarily easy to define. For example, would the manufacturer or software developer bear primary responsibility, or what apportionment could be given

3 Peppet, Scott, Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent, 93 Tex. L. Rev. 85 2014-2015.
4 http://h30499.www3.hp.com/t5/Fortify-Application-Security/HP-Study-Reveals-70-Percent-of-Internet-of-Things-Devices/bap/6556284#.VVAuMPmqpBd
5 FTC Staff Report, internet of things, Privacy & Security in a Connected World, January 2015.
6 Peppet, Scott, Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent, 93 Tex. L. Rev. 85 2014-2015.
7 Brill, Julie, The Internet of Things: Building Trust and Maximising Benefits Through Consumer Control, 89 Fordham L. Rev. 205.
8 http://www.fischer.senate.gov/public/_cache/files/2b3ad47d-f4df-4cb8-b6e3-877de18be0a8/ern15061.pdf.

to the consumer if he/she had failed to adequately protect the IoT device/system by not updating security software or using strong passwords?

INTERNATIONAL AGREEMENTS

On a global scale, the US is spearheading a number of international treaties including the Trans-Pacific Partnership Agreement (***TPP***) (now consented to by Australia), the Trade in Services Agreement (***TISA***) and the Transatlantic Trade and Investment Partnership (***TTIP***) which may impact the way information flowing across jurisdictional boundaries is handled and regulated.

To the extent these international agreements promote the flow of Australian data offshore, the previously discussed concerns regarding cybersecurity and privacy are exacerbated given the limited ability to control what another jurisdiction does with the data.

MANDATORY DATA RETENTION

Under the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth), telecommunications carriers, carriage service providers and internet service providers have to provide certain data to certain government bodies and agencies on request and retain this data for two years.

The mandatory data retention laws apply to telecommunications data including the type and time of a communication (e.g. when an email is sent), the size of a communication, what service was used to transmit the communication (e.g. mobile, landline, email, VoIP, http etc), the address the message was sent to and from, and the location of the device used. The laws do not apply to the content of communications, a user's web browsing history or login information. Industry is presently developing a matrix of specific data types in consultation with government as part of the implementation of the new laws.

The data retention laws apply to carriage services delivered by the carriage service provider. Therefore, many aspects of the M2M (machine to machine) communications involved in IoT applications may be captured by these laws. Whilst government bodies will not be able to access the content of these communications except for metadata (at least without a warrant), they will be able to tell when, how and to whom these communications have been made. This raises the question whether the cost and privacy implications of retaining IoT metadata lead to any tangible law enforcement outcomes or benefits.

DISCRIMINATION AND THE DIGITAL DIVIDE

The aggregation and profiling of user data may lead to marginalisation and create new opportunities for digital discrimination. "Sensor fusion" i.e. the ability to combine information from two disconnected sensing devices to create greater and more complex information[9] can lead to data controllers profiling users based on an infinite number of characteristics e.g. race, gender, level of activity, employment, economic status etc.

This can lead to users being faced with highly targeted and predatory marketing tactics that prey on a user's identified behaviours, patterns and preferences. For example, people in financial difficulty may be approached by financial institutions offering them finance at high interest rates, when they can least afford it.

People who do not use the IoT (e.g. elderly or the poor) may also find themselves increasingly sidelined. For example, in Boston, a mobile app that identified pot holes on a city's roads through the mobile phone's accelerometer and GPS data, helped the city's Public Works Department isolate problem areas and concentrate its resources. However, given the poor and elderly may be less likely to download the app, there were concerns the city's services could be diverted away from the areas that need most attention in favour of younger and wealthier neighbourhoods.[10]

It is clear that the information that can be harnessed by the IoT can be of enormous value, but measures must be put in place to ensure that no matter how well intentioned, the information does not lead to unintended consequences contrary to public policy.

Another consideration for consumers is the extent to which they can easily and cheaply transfer their data from one service provider to another. Over time the quality and quantity of information gathered by one service provider may be of such value to a consumer that he or she wants to transport it to another provider e.g. health, security or financial information. The potentially anti-competitive behaviour of a service provider could be a deterrent to that transfer.

CONCLUSION

The IoT raises a number of regulatory issues that must be counterbalanced with the need to promote and encourage the innovation of the IoT. The EU and US are currently monitoring the emergence of the IoT environment, recognising that enacting legislation whilst the IoT is in is infancy is premature.

In Australia, the existing regulatory framework needs careful review to ensure it is best placed to cope with the enormous growth of the IoT that is forecast. The role of industry also needs to be defined to ensure that the overall response to the technological developments strikes the appropriate balance between innovation and consumer protection.

JAMES HALLIDAY is a partner and REBEKAH LAM a lawyer at Baker & McKenzie. This article represents the personal view of the authors and is not necessarily representative of the views of any client of the firm.

9 Peppet, Scott, Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent, 93 Tex. L. Rev. 85 2014-2015.

10 Finch, Kelsey and Tene, Omer, Welcome to the Metropticon: Protecting Privacy in a Hyperconnected Town, 41 Fordham Urb.L.J. 1581 2013-2014.

Profile: Christina Allen

General Counsel of Fox Sports Australia

CAMLA Young Lawyers representative, Eli Fisher, recently caught up with Christina Allen, to discuss her role as General Counsel of Fox Sports Australia and her views on the key issues facing the industry.

Christina, on behalf of the readers of the CLB, thanks for making the time to speak with us. Perhaps let's start with where you work, and your role in the organisation?

I work at Fox Sports Australia where I have a few different roles within the organisation. I am the General Counsel which means I am the leader of the Legal & Regulatory team which consists of 8 lawyers including myself and a secondee from one of the law firms we use. The team looks after a very broad range of matters including sports rights contract negotiations, music licensing, responding to customer feedback, employment law, contracts for on-air talent, production, outside broadcasts and our technical infrastructure as well as regulatory compliance. I am also the company secretary of Fox Sports Australia and its subsidiaries which involves attending board meetings, preparing board papers for our board and overseeing the company's corporate compliance program. I am also a member of the company's senior executive team and the Legal & Policy Committee for ASTRA, our industry body.

Where have you worked previously, and what led you to your current role?

It's been quite a while since I have worked anywhere else. I joined Fox Sports just before the start of the Sydney Olympics in 2000. This was the perfect time to start a new job at an Australian sports broadcaster as I spent the first month attending various events and functions for the Games which was very exciting. When I first started at Fox Sports, my title was Corporate Counsel and then I was promoted to Manager – Legal & Business Affairs in 2003. I became General Counsel and joined the executive team in July 2011.

Prior to Fox Sports, I had a brief 12 month stint as the first in-house lawyer in Australia for Encyclopaedia Britannica as they planned to re-invent themselves as the "thinking person's" Yahoo! Sadly the dot-com crash hit in April 2000 and many of the staff that had been employed as part of this quest were made redundant including me. Nevertheless it gave me my first taste of working in-house and I haven't looked back.

I started my legal career at Tress Cocks & Maddox (now known as Tresscox) initially as a paralegal and then solicitor in the Insurance & Commercial Litigation team. I couldn't see myself being a great litigator so I begged my supervising partner at the time to let me transfer to the Entertainment & Media team as I had a strong desire to pursue my career in this area, as it was a dynamic and emerging area of law at the time. My boyfriend (and now husband) also worked in the entertainment industry so I knew a bit about it. I worked on various matters for clients in the music, film and television industry including Fox Sports, EMI Music Publishing, XYZ Entertainment and East Coast Pay TV. That's where I first met Patrick Delany who is now my boss today.

What do you consider to be some of the most interesting and challenging aspects of your role?

What I love about working at Fox Sports is that you never know what is going to come across your desk each day. Even after 15 years, I still have matters come up where I say "wow, we haven't done this before" and I need to think outside the square about how we can make it work to meet Fox Sports' commercial and operational objectives while still ensuring that we have a legally compliant framework in place.

Often this has to happen within very tight timeframes as was the case with perhaps the most interesting and challenging matter of my career to date – Fox Sports' recent deal with the Australian Rugby League Commission for the NRL rights which was announced in late November. This involved a number of sleepless nights for me and my team as we bunkered down in the offices of Clayton Utz to negotiate and paper the deal in a very short space of time. Fortunately we also had the support of Gavin Smith and his team from Allens who pushed through with us right to the very end. It was an incredibly intense time for all parties involved but also very rewarding for me and my team to have played a part in securing the biggest sports rights deal in Fox Sports' history.

As with any in-house role like mine, I also look after a range of legal issues that are not related to sports rights or media law. Employment matters come up regularly for me, especially as a member of the senior executive. Another example of a somewhat left of field matter for me involved Fox Sports' construction and relocation to a new building a few years back. I am no expert in construction law, but I had to oversee the legal aspects of the construction of our new building and broadcast facility in Artarmon. I spent many hours locked in board rooms where I was the only female negotiating with the builders and developers and their lawyers. That was certainly a challenge as not only did I not know much about construction, planning and development law and contracts, but I was also heavily pregnant at the time!

Transitioning from a manager of the legal function to becoming the leader of the legal function has been, and continues to be, another interesting challenge. We have recently had 2 new lawyers join our team which means I can now let go of more of the day-to-day legal and transactional work that I have done for a very long time and focus more on the strategic function of General Counsel

by working with my team to ensure that they are a high performance, strongly-engaged team that is able provide true value to our business.

Probably most challenging of all in what I do however is being a full-time working mum with two small children - I could not do what I do in my role without the support of my husband. I just wish he would learn how to stack the dishwasher properly!

What are some of the big legal and regulatory issues facing your industry?

I cannot answer this question without mentioning the anti-siphoning scheme under the *Broadcasting Services Act*. I've lived and breathed it for 15 years. Fox Sports obviously accepts that there needs to be some sort of scheme; but it does need to be reformed given that the broadcast sector is undergoing significant transformational change. The reforms should be wrapped up in the reforms to various media laws that are currently under consideration. Sensible reform in the area will level the playing field for all participants in the industry (by which I mean the entire Australian media industry, not just pay and free-to-air TV.)

Another issue is online piracy. It is essential that we make sure that Fox Sports is able to take advantage of the recent changes to the *Copyright Act* that have been implemented to combat online piracy. But much of the battle in combatting online piracy doesn't necessarily take place in the Courts. We work closely with various sporting bodies to work on ways to protect the rights they grant to us, and there still remains a fair amount of advocacy work to be done in the policy area. The new site blocking provisions will be useful to a degree, but the protection of live sports from piracy raises different issues to the protection of, say, pre-recorded television shows, music or movies – and we need to be very active in the copyright policy space to protect the live sports content in which Fox Sports invests heavily to not only acquire but also produce.

Are you naturally passionate about sport, or is it an area that you fell into?

I've always been interested in sport. I have 4 older brothers who are all very passionate about sport, particularly rugby union, cricket, surfing and skiing – so I really had no choice but to develop an interest in sport growing up. But honestly, when I first started working at Fox Sports it wasn't an all-consuming obsession like it is for many people I work with. In fact, I was actually a little apprehensive about specialising in sport, because my interest in media law was broader than that. But I'm very glad I did. And, as it turns out, a range of other sports have come to grow on me over the course of my time here. I now feel that having a passion about sport is a key criterion when recruiting new members to join my team. Sport is what we do; it's the essence of our business. And a good lawyer at Fox Sports will have a keen understanding of how sport works, and how it is consumed.

What challenges does the current multimedia and digital environment create for FoxSports?

One challenge is the increased competition for sports rights, both from the FTA broadcasters and from emerging online players. The FTA broadcasters have become more active in acquiring sports rights as they are able to now utilise their multi-channels for events that they would not normally show on their primary service. And, with regard to emerging online players, the recent acquisition by Optus of the rights to the English Premier League is an interesting play, as it clearly highlights the importance of live sports programming in order to become an active player in the digital content space and drive customer growth for the rest of their business. I suspect we'll see lots more of that from these online players in the near future.

These developments also present another challenge for Fox Sports – we constantly need to keep ahead of advances in technology and innovate the way we deliver content to our customers – which is obviously essential for a world-class broadcaster to differentiate itself from its competitors – but we also need to navigate how the law applies to those developments, which can be difficult in a cutting-edge environment, especially as the law always seems to be lagging behind. The traditional distribution business models and how they are regulated will not be sustainable in the long term future.

What are some tips for young lawyers looking to work in media law?

First and foremost, I would say, if you are looking to work in media law in particular, then persevere, and be bold. If you're currently in an area of law that you can't see yourself working in for your entire career – like I was – then pick a firm or a company that you would like to work for. Don't be afraid to make contact with the General Counsel or a particular partner with whom you want to work. Persistence generally pays off - contact them on LinkedIn, and make yourself known and they might even agree to have a coffee with you.

If you're lucky enough to score an interview for your dream job, do your research and be enthusiastic about the business and what they do. This is true, of course, for individuals looking for all sorts of roles. But when you apply for a job at a media organisation that specialises in a particular area, you absolutely need to love and understand their content. Sport is what we do, so being passionate about sport (and not just about media or IP law) is fundamental. The same applies with news, movies, music and so on. Become familiar with the developments in the industry. It's such a vibrant and dynamic field, so just reading the newspaper on a daily basis – and following news about regulatory changes, media reforms, rights acquisitions and the like can be really important.

And finally, a word of warning, working in-house in media is not always as glamorous as you might think. Yes, there might be opportunities to take a selfie in the back of a limo on the way to the AFL Grand Final (note my photo!) or to stand on the hallowed turf of the Sydney Cricket Ground sipping a glass of bubbles while you watch your name flash up on the scoreboard at a gala employee recognition dinner - but in order for those opportunities to arise, there will be work that you will need to do that is just not that interesting or exciting, just like working for any other company. So once you score that great job in-house be prepared to roll up your sleeves and get your teeth stuck into whatever work may come across your desk, no matter what the subject matter. You will be rewarded for it in the long run.

Eli Fisher is a lawyer in Sydney at Banki Haddock Fiora.

Punting on the Law:
In Play Betting

Martin Ross and Mark Lebbon provide an overview of the operation of the Interactive Gambling Act 2001 (Cth) and consider the scope of the recently announced review into the Act and the implications for online in play betting.

In early September the Federal Government announced a review into the *Interactive Gambling Act 2001* (Cth) (***Act***). Although the review has been established to address illegal offshore wagering, the terms of reference have been left deliberately broad. This should allow the review to look more generally at the provisions of the Act in the context of the various technological advancements which have occurred since the Act first came into force.

betting online is not allowed on the outcome of, or contingency in, a sporting event where the bets are placed, made, received or accepted after the beginning of the event.

PROHIBITION ON IN PLAY BETTING

The Act regulates access to gambling via a number of platforms, including the internet. More specifically, the Act makes it an offence to provide an 'interactive gambling service' to customers in Australia.[1]

Under the Act, online wagering on sporting events, by registered wagering service providers, is generally allowed as a form of 'excluded wagering service'.[2] However online wagering is not permitted on 'in play' or live aspects of a sporting event. That is, betting online is not allowed on the outcome of, or contingency in, a sporting event where the bets are placed, made, received or accepted after the beginning of the event.[3]

Therefore, a person cannot provide a service offering gambling (online) on any aspect of a sporting event after the event has begun.

For example, an interactive gambling service that enables a bet to be placed on the result of a cricket match after the first ball has been bowled would be prohibited under the Act, as would placing a bet on the player who is going to serve the next ace in a tennis match which has already begun. However, the prohibition would not prevent online bets being placed on the outcome of a tournament or series of matches after the first match within that tournament or series has begun.[4]

The distinction between wagering on the result prior to the commencement of the sporting event and in play was made on the basis that in play betting 'could evolve into highly addictive and easily accessible forms of interactive gambling'.[5]

Importantly, the definition of 'interactive gambling service' also specifically excludes telephone betting services, meaning that in play betting over the telephone is allowed.[6]

The maximum penalty for offering an interactive gambling service is $360,000, however a person who contravenes the prohibition is guilty of a separate offence for each day during which the contravention continues, meaning fines could run into the millions of dollars for breaches over a sustained period of time.[7]

It is also an offence to publish an advertisement for a prohibited interactive gambling service.[8] However, this does not mean the publication of 'live odds' online is prohibited in Australia. Live odds can be published online to allow non-online live wagering on sporting events. For example, during a sporting event, the website of a wagering service provider can display the live odds for that match to facilitate wagering by telephone services.

IN PLAY BETTING OVER THE INTERNET

The distinction made in the Act between betting over the internet and betting by telephone is controversial.

1 Section 15 of the *Interactive Gambling Act 2001* (Cth).
2 Sections 5(3)(aa) and 8A of the *Interactive Gambling Act 2001* (Cth).
3 Section 8A(2) of the *Interactive Gambling Act 2001* (Cth).
4 Supplementary Explanatory Memorandum, Interactive Gambling Bill 2001 (Cth) 11.
5 Supplementary Explanatory Memorandum, Interactive Gambling Bill 2001 (Cth) 10.
6 Section 5(3) of the *Interactive Gambling Act 2001* (Cth).
7 Section 15(2) of the *Interactive Gambling Act 2001* (Cth).
8 Section 61EA of the *Interactive Gambling Act 2001* (Cth).
9 *Betfair Pty Ltd v Racing New South Wales and Another* (2010) 268 ALR 723, [56].

Justice Perram, of the Federal Court, has noted that '[f]or reasons which are not altogether clear the Interactive Gambling Act 2001 (Cth) prohibits betting on events which are "in play"…where the bets are placed via the internet but not where they are placed via the telephone'.[9]

William Hill has recently introduced a product which allows customers placing in play bets using a form of internet technology. William Hill's product (which had previously been branded as "Click to call") allows punters to place bets via automated voice technology without having to make a phone call in the traditional sense. The technology allows customers to place a bet with the click of their mouse, with the only requirement being that that the microphone on the customer's computer or mobile device is switched on.

An investigation was undertaken into the way William Hill conducts wagering on live sport by the Australian Communications and Media Authority (***ACMA***) who referred the matter to the Australian Federal Police (***AFP***). While the AFP declined to investigate, ACMA has stated that it 'remains concerned about the potentially prohibited internet gambling content complained of'.[10] William Hill maintains that its service does not breach the provisions of the Act.[11]

REVIEW

The Federal Government's current review is likely to consider whether the Act should allow punters to place in play bets via the internet, as well as over the telephone. Hopefully the review will provide some clear direction about the future legality of online in play betting.

The recommendations of the review are expected to be provided to the Federal Government in mid-December.

MARTIN ROSS is a Partner & MARK LEBBON a Senior Associate at Hall & Wilcox.

an interactive gambling service that enables a bet to be placed on the result of a cricket match after the first ball has been bowled would be prohibited under the Act

10 Perry Williams, 'Tom Waterhouse wins betting battle with regulators', *The Sydney Morning Herald* (Sydney), 28 October 2015 <www.smh.com.au/business/tom-waterhouse-wins-betting-battle-with-regulators-20151028-gkkkri.html>

11 Marc Moncrief, 'In-play betting: is the law being broker and how much will it cost', *The Age* (Melbourne), 17 September 2015 <www.theage.com.au/victoria/inplay-betting-is-the-law-being-broken-and-how-much-will-it-cost-20150917-gjou6r.html>.

CONTRIBUTIONS & COMMENTS

Contibutions and Comments are sought from the members and non-members of CAMLA, including features, articles, and case notes. Suggestions and comments on the content and format of the Communications Law Bulletin are also welcomed.

Contributions in electronic format and comments should be forwarded to the editors of the Communications Law Bulletin at editor@camla.org.au or to

Valeska Bloch or Victoria Wark

C/- Allens
Deutsche Bank Place
Corner Hunter & Philip Streets
SYDNEY NSW 2000

Tel: +612 9230 4000
Fax: +612 9230 5333

CAMLA contact details:

Email: camla@tpg.com.au
Phone: 02 42 948 059
Mail: PO Box 237,
KINGSFORD NSW 2032

About CAMLA

The Communications and Media Law Association Incorporated (CAMLA) brings together a wide range of people interested in law and policy relating to communications and the media. CAMLA includes lawyers, journalists, broadcasters, members of the telecommunications industry, politicians, publishers, academics and public servants. Issues of interest to CAMLA members include:

- defamation
- broadcasting
- copyright
- advertising
- information technology
- freedom of information
- contempt
- privacy
- censorship
- film law
- telecommunications
- the Internet & online services

In order to debate and discuss these issues CAMLA organises a range of seminars and lunches featuring speakers prominent in communications and media law policy.

Speakers have included Ministers, Attorneys-General, members and staff of communications regulatory authorities, senior public servants, executives in the communications industry, lawyers specialising in media and communications law, and overseas experts.

CAMLA provides a useful way to establish informal contacts with other people working in the business of communications and media. It is strongly independent, and includes people with diverse political and professional connections. To join CAMLA, or to subscribe to the Communications Law Bulletin, complete the form below and forward it to CAMLA.

Disclaimer

The Communications Law Bulletin is the journal of the Communications and Media Law Association which is an independent organisation which acts as a forum for debate and discussion and welcomes the widest range of views. The views expressed in the Communications Law Bulletin and at CAMLA functions are personal views of the respective authors or speakers. They are not intended to be relied upon as, or to take the place of, legal advice.

For further information:

Visit the CAMLA website at www.camla.org.au for information about CAMLA, CAMLA seminars and events, competitions and the Communications Law Bulletin.

To: The Secretary, camla@tpg.com.au or CAMLA, Box 237, KINGSFORD NSW 2032
Phone: 02 42 948 059

Name:

Address:

Telephone: **Fax:**

Email:

Principal areas of interest:

I hereby apply for the category of membership ticked below, which includes a Communications Law Bulletin subscription, and enclose a cheque in favour of CAMLA for the annual fee indicated:

☐ Ordinary membership $130.00 (includes GST)

☐ Corporate membership $525.00 (includes GST)
(include a list of names of individuals - maximum 5)

☐ Student membership $45.00 (includes GST)
(include undergraduate full time student card copy)

☐ Subscription without membership $150.00
(includes GST) (Library subscribers may obtain extra copies for $10.00 each + GST and handling)