LexisNexis

# Internet Law Bulletin

2015 . Vol 18 No 9–10

## Contents





*Information contained in this newsletter is current as at December 2015*

LexisNexis Butterworths

# How Google AdWords campaigns may land businesses in legal hot water under Australian law

***Jamie White*** *POD LEGAL*

## Introduction — how Google AdWords works

This article considers the extent to which Google AdWords can amount to misleading and deceptive conduct, trade mark infringement and passing off under Australian law.

AdWords is an advertising service, which is integrated into Google's search engine service. It allows for "sponsored links" to appear in response to a Google user's search request, either above or alongside the positioning of the "organic search results".

Whereas organic search results are links to webpages that appear in order of relevance to the keywords entered by the user, sponsored links are advertisements, triggered by the same keywords.[1]

Under the AdWords system, advertisers nominate keywords that when searched will cause a link to their webpage appear as a sponsored link. The most popular keywords are "bid" upon by advertisers in a real time auction.

Advertisers bid based on the monetary amount that they are willing to pay each time a user clicks on their advertisement. The closer to the highest bid they are for a particular keyword, the higher up on the search engine page the link to their website will appear. This is subject to a "quality score", which is given by Google according to the relevance of the advertisement and amount of clicks it has previously received.[2]

It is important to note at the outset that *the advertiser* determines both the content and the keywords associated with their advertisement. As is discussed, this point has a significant influence on who bears the liability in terms of potential misleading and deceptive conduct, trade mark infringement and the common law tort of passing off.

## Key points

- The purposes of protecting consumers, property and goodwill respectively yield different legal inquiries into each of these areas.
- The advertiser, rather than Google, is more likely liable for misleading and deceptive conduct, trade mark infringement, or passing off.
- Trade mark infringement will only be made out in limited circumstances in Australia.
- Passing off will be made out in even more limited circumstances.

## Tips for practitioners

- Try to discourage clients from including the names of other businesses or trade marked names in the headlines of AdWords advertisements.
- Note that using companies' names and trade marks as keywords in an AdWords campaign may contribute to a finding of trade mark infringement or passing off, but is less likely, of itself, to constitute misleading and deceptive conduct.
- If infringement is made out, then the onus will fall on your client (unless your client is Google). Therefore, it is worth performing trade mark searches and other due diligence checks before embarking on AdWords campaigns, especially since intention is not a consideration for the imposition of liability on your clients.

## Misleading and deceptive conduct

Section 18 of the Australian Consumer Law (ACL) provides that a person must not, in trade or commerce, engage in conduct that is misleading or deceptive or is likely to mislead or deceive.[3]

Advertisements placed through Google's AdWords system may result in misleading and deceptive conduct through the use of certain keywords or advertisement headlines which are exclusively associated with another person or business. For example, the name of that other person or business.

A leading example is a 2011 case, where Trading Post Australia Pty Ltd (Trading Post) was found to have engaged in misleading and deceptive advertisements by

causing certain advertisements to be displayed on Google via AdWords.[4] Trading Post selected the names of several competitor businesses as the keywords, which would trigger its own advertisements. Further, the headline of the advertisement was the name of the competitor business. To illustrate, in the case of Kloster Ford, one of Trading Post's competitor businesses, the advertisement displayed was as follows:

> "Kloster Ford
> www.tradingpost.com.au New/Used Fords —
> Search 90,000 + auto ads online. Great finds daily!"[5]

Justice Nicholas found that because the Trading Post's URL was displayed within this advertisement and other similar advertisements, the ordinary and reasonable members of the class of people to whom the advertisement was directed would appreciate that it would take them to Trading Post's website.[6]

His Honour continued, however, to say that this advertisement and others made the following misleading representations:

- there was an association or affiliation between Trading Post and Kloster Ford, which did not exist;[7] and
- information regarding Kloster Ford and Kloster Ford car sales could be found at Trading Post's website, which was incorrect.[8]

This provides an idea of what might constitute a "definitely in" example of misleading and deceptive conduct by an advertiser using AdWords.

However, the important question remains of whether Google itself, as the agent facilitating the production of these advertisements, can be liable for misleading and deceptive conduct.

Nicholas J, applying *Butcher v Lachlan Elder Realty Pty Ltd (Butcher)*,[9] reasoned that:[10]

> Whatever representation the vendor made to the purchasers by authorising the agent to issue the brochure, it was not made by the agent to the purchasers. The agent did no more than communicate what the vendor was representing, without adopting it or endorsing it.

The High Court has endorsed this view in a later case taken up by the Australian Competition and Consumer Commission (ACCC) against Google itself, adding some context to its reasoning.[11] In this case, the High Court considered a series of advertisements similar in nature to the Trading Post advertisements, made by a number of different advertisers.

In a joint judgment, Chief Justice French and Justices Crennan and Kiefel reasoned:[12]

> That the display of sponsored links (together with organic search results) can be described as Google's response to a user's request for information does not render Google the maker, author, creator or originator of the information in a sponsored link … Google is not relevantly different from other intermediaries, such as newspaper publishers (whether in print or online) or broadcasters (whether radio, television or online), who publish, display or broadcast the advertisements of others … To the extent that it displays sponsored links, the Google search engine is only a means of communication between advertisers and consumers.

In separate judgments, Justice Hayne substantially agreed with the majority, and Justice Heydon found that placing liability on Google in this case would create "an exceptionally wide form of absolute liability for those who publish information in the media".[13]

## Takeaway points:

- If liability for misleading and deceptive conduct falls on anybody in an AdWords context, it will be the advertiser, and not Google.
- Similarly, there is no practical difference between Google's AdWords and the paid advertising offered by hard copy newspapers.
- Misleading and deceptive conduct need not be intentional, but rather "likely to mislead or deceive", therefore conducting trade mark searches and other due diligence before embarking on an AdWords campaign would be advisable.
- The courts recognise the nuance involved in advertisements created using AdWords, and the intelligence of the consumer. Therefore, the more blatantly fraudulent attempts at navigating the AdWords system, such as that in the *Trading Post* case, will be caught out because they are likely to mislead or deceive the consumer. However, using more peripheral search terms, which are not the names of businesses, will not necessarily be considered misleading and deceptive, because the user of the Google search engine will be unlikely to believe the underlying representations of the advertisement.
- Google has begun to do its part to reduce this behaviour. It has a Trade mark policy,[14] which allows owners of trade marks to complain about the use of their trade marked name. Further, the quality score function, which promotes the most relevant websites in the order of sponsored links, and that appears in response to a search request, makes it less likely that a consumer will click on an advertisement. However, this does not prevent it from being misleading or deceptive.

## Trade mark infringement

Google does not prevent businesses from bidding on words which are protected by trade mark law in certain jurisdictions. It would be unrealistic to expect Google,

an international company, to periodically search every trade mark database and ensure that the words upon which people make bids are not protected as trade marks. Instead, Google has a *Trade mark policy*, which allows trade mark owners to complain to Google, who may respond by placing restrictions on the people who may bid on the trade marked word or words.[15]

Google will not restrict the use of trade marked material if it is used by resellers or informational websites, or where the use is authorised by the owner of the relevant trade mark. Further, Google permits the use of trade marked material in advertisements if either:[16]

- the ad[vertisement] text uses the term descriptively in its ordinary meaning, rather than in reference to the trade mark; or
- the ad[vertisement] is not in reference to the goods or services corresponding to the trade marked term.

Unlike misleading and deceptive conduct, Australian courts have yet to consider whether use of a registered trade mark as a keyword for the purposes of an AdWords advertisement amounts to trade mark infringement under the Trade Marks Act 1995 (Cth) (Trade Marks Act).

However, as discussed in relation to misleading and deceptive conduct, the liability rests on the advertiser for using the names of other businesses in the headline of its advertisements. It is likely that this holds true for trade mark infringement. Intuitively, the same reasoning could be applied to a case of trade mark infringement because the same parties are acting in the same way; it is the interest being protected that is different.

The United Kingdom's High Court of Justice has considered this question. In *Interflora Inc v Marks & Spencer Plc (Interflora)*,[17] a company called Marks and Spencer used the name "Interflora", which was a word subject to the registered trade mark of Interflora Inc, as a keyword in an AdWords campaign. Marks and Spencer **did not** include "Interflora" in the text of its advertisement. It was held that this constituted trade mark infringement on the behalf of the advertiser because the sponsored links may have led the "average reasonably well-informed and reasonably attentive internet user" to believe that Marks and Spencer was part of the Interflora network. However, this decision has been appealed and remitted to the High Court of Justice on the grounds that there was insufficient evidence for the judge to make the findings that he did in this case.[18]

It is unlikely that this would extend to Australian trade mark law.

In Australian law, trade marks are used to identify a unique product or service and distinguish it from those provided by other traders. Under the Trade Marks Act, a trade mark may be any combination of (*inter alia*) letters, words, names, numerals, brands and colours, which are used to distinguish goods or services provided in the course of trade by a person from those provided by other people.[19]

A person's trade mark can be infringed in a number of ways. Relevantly, a person infringes a registered trade mark if the person uses, as a trade mark, a sign that is substantially identical with, or deceptively similar to, the trade mark in relation to goods or services in respect of which the trade mark is registered.[20]

Importantly, the infringer must use the trade mark "as a trade mark", which is to say that the trade mark of one company must be used by another, as a sign used to distinguish its own goods and services from those of other companies.

By contrast, under the United Kingdom's Trade Marks Act,[21] the infringer must use the trade mark "in the course of trade".[22] This is vastly broader than the Australian provision, and therefore likely covers the case of *Interflora*.

Therefore, in Australia, using another company's trade mark in any capacity will unlikely constitute trade mark infringement, unless it is used *as a trade mark*.

This line of reasoning was supported in 2010 in *Mantra Group Pty Ltd v Tailly Pty Ltd (No 2) (Mantra Group)*,[23] when Justice Reeves reasoned that the infringer must use the mark as a "badge of origin" in the sense that it indicates a connection in the course of trade between goods or services and the person who applies the mark to those goods or services. His Honour found in this case that Tailly's use of Mantra Group's registered "Circle on Cavill" apartment complex trade mark in a number of internet contexts, including AdWords, constituted trade mark infringement.[24]

This means that use of a trade mark as a key word in an AdWords campaign can constitute trade mark infringement, provided it is used *as a trade mark*. It is unclear whether the mere use of a trade mark as an AdWords keyword may amount to infringement but what the *Mantra Group* case makes clear is that it can certainly be a contributing factor.

## Takeaway point:

- Only in specific circumstances, where one person uses another person's trade mark *as a trade mark*, will infringement be made out in Australia.

## Passing off

Trade marks that are not registered pursuant to the Trade Marks Act may be protected under the common law tort of "passing off". The tort of passing off is based on the principle that nobody should represent that their goods or services are those of another, and comprises three elements that must be made out:

1) that the plaintiff has an established goodwill in the material which the defendant is using and of which the plaintiff complains;
2) that the defendant misrepresents that its goods and/or services are those of the plaintiff as a result of which the relevant consuming public will be deceived; and
3) that the plaintiff has suffered or will suffer damage as a result of that action.[25]

These elements were set out in the late 1800s, so have since grown considerably to cover almost all situations of commercial dishonesty, including making an implication.

An action in passing off may be run instead of a breach of s 18 of the ACL because an account for profits is an available remedy, which may not be available under the ACL.

Passing off has only had peripheral judicial consideration in respect of AdWords. In the *Trading Post* case, Nicholas J noted that there are fundamental differences in the underlying purpose between s 18 and passing off. Whereas the ACL is directed at consumer protection, passing off is directed at the protection of goodwill. He continued to note the difference between the test of whether a representation is likely to damage the reputation in a particular "get-up or name" and whether a representation is itself misleading.[26]

Arguing from this distinction, in an action for passing off, the act of misleading representation must cause the harm complained of. So, the stronger the causative link between the damage to a party's goodwill, the more likely that a case of passing off will be made out.

Intuitively, this draws the analysis in an AdWords context closer to that of the trade mark infringement rather than misleading and deceptive conduct. If a person uses another person's trade mark *as a trade mark*, it is more likely to damage goodwill than if it is not used as a trade mark.

Arguing from first principles, if one person outbids another person on AdWords for their unregistered trade mark, it is likely for there to be damage done to the first person's goodwill if they cede their position in the order of priority of sponsored links.

## Takeaway point:

- To show that a person has engaged in activities constituting passing off through the use of AdWords it is necessary to show a causal nexus between the use of AdWords and damage to goodwill.

## Conclusion

The consistent trend between all three of the above bodies of law is that liability will rarely, if ever, fall upon Google for misleading uses of the AdWords service by an advertiser. It is important for intellectual property lawyers to be mindful that the focus of each misleading and deceptive conduct, trade mark infringement and passing off is different.

Misleading and deceptive conduct is based on consumer protection and therefore the focus of the inquiry is whether the consumer would be misled by certain representations. Trade mark infringement is concerned with protecting property rights, and finally, passing off is concerned with protecting goodwill. It is important to remember that each of these distinct areas of focus guide the legal inquiry to be undertaken and, therefore, what you need to be wary of when advising clients on the use of Google AdWords campaigns.

***Jamie White***
*Solicitor Director*
*Pod Legal*
*Jamie@podlegal.com.au*

## Footnotes

1. *Google Inc v Australian Competition and Consumer Commission (ACCC)* (2013) 249 CLR 435; (2013) 294 ALR 404; [2013] HCA 1; BC201300295 at [22].
2. Econsultancy, *What is Google AdWords and how does it work?*, October 2014, www.econsultancy.com; Wordstream, *What Is Google AdWords? How the AdWords Auction Works*, November 2014, www.wordstream.com.
3. Competition and Consumer Act 2010 (Cth), Sch 2 s 18(1).
4. *Australian Competition and Consumer Commission (ACCC) v Trading Post Australia Pty Ltd* (2011) 283 ALR 310; (2011) 93 IPR 358; [2011] FCA 1086; BC201107288.
5. Above n 4, at [100].
6. Above n 4, at [126].
7. Above n 4, at [130].
8. Above n 4, at [135]–[136].
9. *Butcher v Lachlan Elder Realty Pty Ltd* (2004) 218 CLR 592; (2004) 212 ALR 357; [2004] HCA 60; BC200408200.
10. Above n 4, at [40].
11. Above n 1.
12. Above n 1, at [6,9].
13. Above n 1, at [151].
14. Google, *AdWords Trade mark Policy*, October 2012, www.support.google.com
15. Above n 14.
16. Above n 14.
17. *Interflora Inc v Marks & Spencer Plc* [2013] All ER (D) 238 (May); [2013] IP & T 931; [2013] EWHC 1291 (Ch) (Arnold J) (*Interflora*).
18. Above n 17.

19. Trade Marks Act (1995) (Cth), ss 6, 17.
20. Trade Marks Act (1995) (Cth), s 120(1).
21. Trade Marks Act (1994) (UK).
22. Above n 21, s 10(1).
23. *Mantra Group Pty Ltd v Tailly Pty Ltd (No 2)* (2010) 267 ALR 347; (2010) 86 IPR 19; [2010] FCA 291; BC201001870 at [50] (*Mantra Group*).
24. Above n 24.
25. *Reddaway v Banham* [1896] AC 199; (1896) 1 B IPR 401; (1896) 13 RPC 218 204 (Lord Herschell).
26. Above n 4, at [89].

# The US Digital Millennium Copyright Act: use and concerns in Australia

***Nicholas D Wells*** *KIRTON MCCONKIE*

The Digital Millennium Copyright Act (DMCA) is a section of the United States Copyright Act that provides some unusual tools that may assist Australian copyright owners who battle online infringement. Understanding the DMCA will also benefit anyone who does business with US businesses or consumers.

## Background of the DMCA

In 1998, the United States amended the US Copyright Act to account for two treaties that the US had become a member to.[1] The amendments, known as the DMCA, addressed the problem of circumvention of technological controls intended to prevent copyright infringement (Digital Rights Management or DRM technologies); not only was the production of tools intended to circumvent DRM technologies criminalised, but the act of circumvention was criminalised, even if no copyright infringement resulted. Although these provisions include a number of exceptions, this portion of the DMCA has been controversial from the outset.

Yet the DMCA is more widely known for its approach to another problem facing the world in 1998. Copyright owners were concerned with the growing ease with which digital technologies permitted rapid copying and dissemination of copyrighted works; providers of online services were also concerned that copyright laws would make them liable for the acts of their users who posted or transmitted content that infringed third-party copyrights. In response, the DMCA strikes a statutory bargain that attempts to address the concerns of both sides. Copyright owners can use the DMCA to quickly and easily have infringing content removed with the help of content hosts (online service providers); those online service providers can avoid legal liability for copyright infringement by following the steps in the DMCA, which amount to a safe harbor.

This arrangement is commonly known as the DMCA takedown procedure; notices submitted to an online service provider are known as DMCA takedown notices.[2]

### *The DMCA takedown procedure*

While the DMCA does not apply to Australian businesses, consumers or online service providers, Australian copyright owners can make use of it for any online infringements occurring on US-based websites. Australian businesses may also benefit from understanding DMCA provisions when dealing with US businesses or consumers.

Practically speaking, the DMCA functions as follows:

1. A copyright owner becomes aware of an infringing work that has been made available online. For example, a copyrighted photo is published to illustrate a blog post, or a blog post is re-published on another blog without consent, or a copyrighted video is posted for public viewing.
2. The copyright owner identifies the third-party host of the material. This is normally either the company that operates the website or the hosting company that provides the back-end service to the website operator. Examples of the first include Facebook, YouTube; examples of the second include GoDaddy or BlueHost (equivalent to HostPapa or DigitalPacific in Australia).
3. The copyright owner sends a DMCA takedown notice to the online service provider. This can be sent electronically or as a paper notice, but it must include the following items to be valid:[3]
   a. The signature of a person authorised to act on behalf of the copyright owner.
   b. A clear identification of the copyrighted work claimed to have been infringed.
   c. A clear identification of the material that is claimed to be infringing and information reasonably sufficient to permit the online service provider to locate the material.
   d. Your contact information.
   e. A statement that the complaining party has "a good faith belief that use of the material in the manner complained of is not authorised by the copyright owner."
   f. A statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorised to act on behalf of the owner of the copyright that is allegedly infringed.

4. The online service provider will typically remove access to the material that you are complaining about and must then notify the owner of the page or website where it was located.

5. The owner of the page or website that was taken down has the right to submit a counter-notification that has many of the same formalities as the original notice and states — in summary — that it was a mistake to remove access to the page or site.[4]

6. If a counter-notification is not sent, then the service provider will do nothing and the material remains unavailable (but see the caveats in the sections that follow).

7. If a counter-notification is sent, the online service provider must make the material available once again, unless it receives notice from the copyright owner that the owner has sought a court order regarding the alleged infringing activity.[5]

On the whole, the above process is straightforward, but its purpose is often misunderstood by copyright owners and website operators alike. Contrary to the view of some enraged copyright owners, the service provider does not have a legal obligation to take down the alleged infringing content. Doing so merely allows the service provider to avoid the possibility of legal liability (hence most will follow the procedure above). Indeed, the DMCA includes several provisions expressly stating that a service provider "shall not be liable" if acting in accordance with this law. When I say in item 7, above, that the service provider "must make the material available once again", that is what is needed to comply with the DMCA and thus take advantage of the safe harbor liability shield. But if the service provider decides not to follow the DMCA "rules", it is free to do so.[6]

Similarly, the terms of service used by most service providers do not require that they post any content that they feel is inappropriate or infringing. Thus, even if a service provider does not follow the DMCA rules, they may elect to remove access to material simply to remove themselves from a fight between website operator and copyright owner. (As one attorney for a prominent ecommerce site tersely informed me, they don't have to sell anything they don't want to sell.)

### *Applicability in Australia*

Copyright owners based in Australia can use the DMCA as a low-cost and typically a very quick method of dealing with online copyright infringement.

Online service providers in Australia should also be aware of DMCA notices so that they will understand the intention of US-based copyright owners who may submit DMCA takedown notices. Australian service providers need not comply with such notices but should consider implementing policies commensurate with Australian laws for reviewing and dealing with possible infringements that they learn of.

## Problems with the DMCA

While the DMCA takedown procedure is a clean and simple solution on its face, the implementation has become fraught with practical problems and legal uncertainties during the past 18 years.

### *Overburdened providers and owners*

Online service providers such as Google, Instagram, Pinterest, Facebook and YouTube have automated the processing of DMCA takedown notices. These, and many web hosting companies, provide an online form that copyright owners can use to submit a DMCA takedown notice.[7] Yet the most recent figures indicate that Google received more than 55 million notices in the past month. As discussed below, each requires human review. Such a system is simply not sustainable for service providers.

On the other side, copyright owners — initially pleased with the simplicity of solving online infringements — have learned that serial infringers can move locations almost faster than service providers can disable access to infringing content. The infringers have also learned that sending a counter-notification letter will usually restore access to the infringing content. (Those who are highly skilled at copyright infringement do not blanch at perjury.) The net result is that owners of valuable copyrighted assets also must invest significant resources in a never-ending game of "whack-a-mole", chasing infringers around the digital universe.

As in any field of law, a statutory tool intended to facilitate dispute resolution between two reasonable parties with differing views of the facts cannot adequately deal with intentionally bad actors. That is especially true when the bad actors have at their disposal a range of technological tools for misusing copyrighted content on an enormous scale.

Yet it is not merely serial infringers that have taken advantage of DMCA takedown notices. A study from 2005 found that more than one-half of takedown notices received by Google were from competitors of the alleged infringers and more than one-third were "not valid copyright claims".[8]

### *Additional cautions for copyright owners*

Even when copyright owners have a valid basis for concern and are not dealing with serial infringers, caution is warranted when sending DMCA takedown notices. Indeed, the ease with which they can be used may cause copyright owners to be careless in evaluating their rights, hoping to shift the burden of careful review to others.

Section 512(f) of the DMCA provides that a party may be awarded damages, including attorneys fees, that arise from a knowing, material misrepresentation in a DMCA takedown notice or counter-notification.[9]

It remains unclear just what a "knowing, material misrepresentation" would be, but a long-running case involving Universal Music highlights the concern of copyright owners who fear a much-increased burden of investigation before using DMCA to deal with online infringements.

The principal question that many copyright owners have asked is whether fair use must be considered before sending a DMCA takedown notice. Fair use is an affirmative defense in the US Copyright Act.[10] If found applicable, fair use excuses conduct that would otherwise be deemed infringement, based on factors such as:

- the impact on commercial value of a work;
- the nature of the use; and
- the nature of the work itself.

Yet, as an affirmative defense, only a judge can determine if fair use actually applies in a given case.

### *Recent Ruling in Lenz v Universal Music*

In *Lenz v Universal Music Corp*,[11] a home video posted on YouTube was taken down via a DMCA notice from Universal Music. Lenz first filed suit in 2007, arguing that Universal Music acted in bad faith when it ordered removal of a 29-second video of her baby in which she asserted that the use of a copyrighted song was likely to be permitted as fair use. Last month the latest ruling in the case was handed down from the US Federal Court of Appeals for the 9th Circuit.[12] It affirms earlier rulings in the case stating that a copyright owner must "consider" fair use before sending a DMCA takedown notice.

Yet this ruling leaves questions about what level of investigation is required to avoid liability under s 512(f) for making a material misrepresentation in a DMCA takedown notice. The 9th Circuit did state that consideration of fair use "need not be searching or intensive" and that a computer program that matched online content with copyrighted works appeared to be a valid method of reviewing a high volume of online content.[13]

With this ruling in mind, many copyright owners are now re-evaluating how to document the processes they use to send DMCA notices, including making explicit mention of some minimal analysis of the four statutory fair use factors.

## Conclusion

The DMCA is likely to play an important role for the foreseeable future as copyright owners deal with online copyright infringements. By understanding its procedures and limitations, Australian copyright owners can take advantage of DMCA takedown notices and Australian business owners can understand the context in which their American partners are operating.

***Nicholas D Wells, JD, LLM, MBA***
*Shareholder*
*Kirton McConkie PC*
*nwells@kmclaw.com*
*www.kmclaw.com*

## Footnotes

1. See generally, The Digital Millennium Copyright Act Of 1998, US Copyright Office Summary at www.copyright.gov.
2. 17 US Code § 512 — Limitations on liability relating to material online, available at www.law.cornell.edu.
3. Above n 2, at (c)(3)(A).
4. Above n 2, at (g)(3).
5. Above n 2, at (g)(2)(C).
6. Service providers typically follow DMCA procedures as a means of avoiding secondary liability for copyright infringement; if a service provider does not comply with DMCA procedures, it is likely to be named as a defendant if the copyright owner eventually files a lawsuit. Notwithstanding the liability shield provided by the DMCA, several plaintiff copyright owners have sought to hold service providers liable for direct copyright infringement based on the service provider having "known or should have known" about the infringement taking place on its site. In at least one noteworthy case, the court did not find for the plaintiff on such a claim. See *IO Group Inc v Veoh Networks Inc* 586 F Supp 2d 1132 ND Cal (2008).
7. See for example, the links provided at www.facebook.com, www.about.pinterest.com, www.help.instagram.com and www.support.google.com.
8. Falsified DMCA notices sent by competitors to major (overburdened) sites such as Facebook may cause significant harm to a business and be very difficult to resolve because of the hesitancy of service providers to fully analyse claims or "take sides" in a spurious "copyright dispute" that was actually nothing more than a misrepresentation intended to harm a competitor.
9. Above n 2, at (f).
10. 17 US Code § 107 — Limitations on exclusive rights: Fair use, available at www.law.cornell.edu.
11. *Lenz v Universal Music Corp* 572 F Supp 2d 1150 ND Calif (2008).
12. ND Calif, Docket No 5:07-cv-03783- JF (14 September 2015), available at www.cdn.ca9.uscourts.gov.
13. Above n 13, at [18].

# Mandatory data breach notification in Australia

***Gordon Hughes*** *and* ***Andrew Sutherland*** *ASHURST*

The federal government recently foreshadowed the introduction of a mandatory data breach notification scheme in Australia. In this article, we consider, by way of background, the current law in Australia regarding data breach reporting obligations, past recommendations for reform and previous reform efforts, the benefits that such a scheme could offer and a number of the key features that we expect to see in any future draft legislation.

## The digital economy and the cyber threat

As the digital economy continues to expand organisations are increasingly collecting and storing data, including personal information, electronically. As the range of cyber threats become greater in number, more sophisticated and harder to detect, the risks and potential consequences associated with unauthorised access to, and disclosure of, personal information become increasingly serious.[1] In this environment, the need for improved data security and protection measures has never been more critical, nor has the importance and relevance of mitigation strategies designed to reduce the risks and consequences associated with data breaches.

One such mitigation strategy is a legislated mandatory data breach notification scheme, under which organisations would be compelled to notify affected individuals and the Australian Information Commissioner (Commissioner) about data breaches.[2]

## The current law in Australia regarding data breach reporting

With the exception of certain specific instances relating to health information,[3] there is currently no obligation under Australian privacy and data security law which requires organisations to report data breaches. The practice of reporting such breaches is, however, encouraged. Under Australian Privacy Principle 11, relevant organisations are required to take reasonable steps to protect personal information which they hold.[4]

In April 2012, the Office of the Australian Information Commissioner (OAIC) released a guide entitled *Data Breach Notification — A Guide to Handling Personal Information Security Breaches*. The purpose of the guide is to provide agencies and organisations with guidance when responding to a data breach involving personal information which they hold. The approach recommended by the OAIC is not mandatory in the absence of legislation, but it is useful in clarifying the Commissioner's expectations as to what amounts to a reasonable reaction by an entity subject to the Australian Privacy Principles in any given situation. For example, the Commissioner considers that notifying affected individuals about a data breach where one occurs may be one such reasonable step.[5]

## Previous reform efforts

There have been several previous reform efforts in Australia relating to the proposed introduction of a mandatory scheme. To date, all have been unsuccessful. Senator Stott Despoja introduced the Privacy (Data Security Breach Notification) Amendment Bill 2007 (Cth) into the Senate on 16 August 2007. The Bill lapsed on 12 February 2008. It was subsequently restored, but then lapsed again on 28 September 2010.[6] On 29 May 2013, the Privacy Amendment (Privacy Alerts) Bill 2013 (Cth) was introduced into the House of Representatives. It lapsed on 12 November 2013.[7] The same Bill was then re-introduced into the Senate by Senator Singh on 20 March 2014.[8] While that Bill is still before the Senate, it has not progressed since 19 June 2014, and will presumably lapse in due course as well.

## Past recommendations and benefits of a mandatory scheme

In its watershed 2008 report entitled *For your Information: Australian Privacy Law and Practice*, the Australian Law Reform Commission (ALRC) proposed introducing a mandatory scheme in Australia. The ALRC proposed that:[9]

> The *Privacy Act* should provide for notification by agencies and organisations to individuals affected by a data breach. This requirement is consistent with the *Privacy Act*'s objective to protect the personal information of individuals. Data breach notification can serve to protect the personal information from any further exposure or misuse, and

encourages agencies and organisations to be transparent about their information-handling practices.

The primary justification for introducing a mandatory scheme in Australia is to provide individuals affected by a data breach with an opportunity to take steps to protect themselves and their interests, such as by mitigating the potential consequences of a breach.[10] A mandatory scheme would also likely lead to the dissemination of more detailed information about the privacy and information handling practices of organisations, as noted in the ALRC's above report. This would assist consumers in making informed decisions about the organisations with which they may wish to transact, and disclose personal information to.[11] A mandatory scheme could further be expected to incentivise the taking of active steps by organisations to improve and strengthen their data security defences, given the potential reputational and commercial risks associated with having to report data breaches.[12]

## Back on the agenda

The Parliamentary Joint Committee on Intelligence and Security (JCIS) has from time to time made recommendations concerning the introduction of a mandatory scheme — first in 2013 and then again earlier this year. On both occasions the JCIS made the recommendations in the context of considering proposals that ultimately led to the recent introduction of Australia's controversial data retention regime.[13]

In a joint media release dated 3 March 2015,[14] the Attorney-General and Minister for Communications announced that the Federal Government would support all of the recommendations made by the JCIS in its 2015 report concerning the draft data retention legislation. In relation to the JCIS's recommendation concerning a mandatory scheme, the Attorney-General and Minister for Communications stated that: "The Government agrees to introduce a mandatory data breach notification scheme by the end of 2015, and will consult on draft legislation".[15]

We currently await the release of that draft legislation.

## Key features of mandatory schemes

Various forms of mandatory schemes have been introduced in overseas jurisdictions, including in various states across the US.[16] The key features of these schemes are worth considering in seeking to determine the most practicable and effective design for an Australian mandatory scheme.

For the purposes of managing the burdens imposed on organisations under a mandatory scheme, there are certain key features which we expect to see addressed in any new draft legislation, including the following:[17]

- The nature of the relevant "trigger event" which gives rise to the obligation to notify — key features of this aspect of the scheme concern the degree of harm to the affected individuals flowing from the breach and whether or not an obligation to notify arises in the absence of the relevant organisation being required to make an assessment of, and form a view regarding, the likely risk of such harm occurring.[18]
- The relevant corpus of personal information to which the scheme applies — a key issue in relation to that is whether or not the obligations to notify will only apply in relation to specific categories of information (for example, personal financial information).
- The form and detail required to be included in the data breach notifications and the timeframes available for reporting to occur — the greater the extent and detail required to be included in notifications, the more likely it would be that further investigations would be required and additional costs incurred.
- The inclusion of appropriate exceptions — such as where reporting a data breach would not be in the public interest (for example, where doing so could compromise a criminal investigation or be contrary to national security interests) or where the compromised information was adequately encrypted or digitally redacted. It would be critical for relevant organisations to be able to readily understand the nature and extent of their obligations and the availability and applicability of exceptions in particular circumstances.

For now, as noted above, we await the release of the foreshadowed draft legislation with great anticipation.

**Authors**

***Gordon Hughes***
*Senior Consultant*
*Ashurst*
*gordon.hughes@ashurst.com*

***Andrew Sutherland***
*Lawyer*
*Ashurst*
*andrew.sutherland@ashurst.com*

## Footnotes

1. Australian Cyber Security Centre *Australian Cyber Security Centre 2015 Threat Report*, pp 2, 4–9 and 24. The 2013–2014 Annual Report of the Office of the Australian Information

Commissioner reports that a total of 71 (voluntary) data breach notifications were received in 2013–2014, amounting to a 16.4% increase in comparison to the 2012–2013 period.

2. Parliamentary Joint Committee on Intelligence and Security *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, p 293, para 7.110.
3. Personally Controlled Electronic Health Records Act 2012 (Cth), s 75.
4. Privacy Act 1988 (Cth), Sch 1, s 11.1. See also ss 20Q and 21S of that Act.
5. Office of the Australian Information Commissioner *Data breach notification guide: A guide to handling personal information security breaches* (2014) p 6.
6. Parliament of Australia, Privacy (Data Security Breach Notification) Amendment Bill 2007 [2008], August 2007, www.aph.gov.au.
7. Parliament of Australia, Privacy Amendment (Privacy Alerts) Bill 2013, May 2013, www.aph.gov.au.
8. Privacy Amendment (Privacy Alerts) Bill 2014 (Cth).
9. Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice (ALRC Report 108)*, s 51.73.
10. Above n 9, ss 51.76, 51.78; Information Policy Institute *Towards a Rational Personal Data Breach Notification Regime* (2006), 3. The potential consequences of a data breach are not confined to financial harm either as personal information includes health information and the unauthorised disclosure of health information may lead to discrimination and/or reputational damage.
11. Above n 9, s 51.81.
12. Above n 10, s 51.80.
13. Under that regime, which commenced on 13 October 2015, a large number of organisations, including internet services providers and telecommunications services providers will be obligated to collect and retain detailed metadata concerning a range of communications made or received by their customers for a 2-year period. See the Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 (Cth), Pt 5–1A. See JCIS *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, Recommendation 42 and JCIS *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, Recommendation 38, pp 293–95.
14. Attorney-General for Australia "The Australian Government has responded to the inquiry of the Parliamentary Joint Committee on Intelligence and Security (PJCIS) into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014" media release (3 March 2015).
15. Above n 14.
16. Above n 9, ss 51.4, 51.14. See also, eg, Office of the Attorney General *Data Security Breach Reporting,* www.oag.ca.gov (State of California) and Office of the Indiana Attorney General *Security Breach FAQ's & Notification Form For Businesses,* www.in.gov (State of Indiana).
17. These issues are discussed and reflected in Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice (ALRC Report 108)*, s 51 as well in, for example, the Explanatory Memorandum to Privacy Amendment (Privacy Alerts) Bill 2014 (Cth), pp 2–7.
18. Above n 9, s 51.21–22.

# Evidentiary issues with social media and confessions and admissions

***Paul Venus*** *HOLDING REDLICH*

## Tips for practitioners

- Existing evidentiary principles apply to confessions made on social media. Ensure that you strictly comply with the requirements at Common Law or under the Evidence Act.
- It is necessary to prove that the person who is supposed to have made the confession actually posted the statements that are alleged to be a confession. This can be difficult to prove unless you can lead evidence of the act of a person making a post.
- Authentication of a post may involve reliance on circumstantial evidence. Be aware that the timing of a post, content of a post or context of an exchange of posts may be useful to authenticate it.
- The social media confession must be voluntary, and fair to admit into evidence, just like any other confession.

## Introduction

There is an old proverb that "open confession is good for the soul". Recently, it seems that users of social media have taken this message to heart. Every month, news services report on criminals who have confessed on Facebook. Murder, rape, theft and all manner of socially abhorrent behaviour are paraded on social media.[1] Facebook and other social media sites even have "confession pages", which are meant to enable people to share statements, including confessions on an anonymous basis. Since 2013, many of these pages have gone viral on the internet.

The law relating to confessions is relatively established. A confession is an admission which is a direct and express acknowledgment of facts suggesting guilt. Both at Common Law and under s 81 of the Evidence Act 1995 (Cth), the hearsay rule does not apply to evidence of a confession. However, courts have the discretion to exclude evidence of a confession in certain circumstances.[2] There are a number of legal requirements that must be met before a confession will be allowed as admissible evidence. Once a confession is admitted, the weight which should be attached to the confession is a matter for the jury.

But does the confession made on a social media platform, in a Facebook post, in a tweet or on some other form of medium easily fit within these rules of evidence? The answer is that the existing evidentiary principles that relate to confessions made other than on social media will also apply to social media confessions. But, that being noted, social media does present specific issues that need to be addressed when determining if a post on that media is admissible as evidence of a confession.

## Provenance of the social media post

The first problem that arises with confessions made on social media sites is one of provenance. It is necessary to prove that the person who is supposed to have made the confession actually posted the statements that are alleged to be a confession.

It is always possible that a person did not make a post, and unless someone can give evidence that they saw the person make the post there can be arguments from a defendant that the post was not made. In the absence of an admission that a post has been made by a person, it is necessary to lead evidence to prove the provenance of the post having been made.

It may be possible to prove that a post has been made by leading evidence to show the origin of a post in circumstances where only one person had access to the computer or device on which the post was made.

In 2014 in the Western Australian case of *Dabrowsk v Greeuw*,[3] the defendant to a defamation case denied making a post on a Facebook page. She claimed that she had typed the words for the post but not posted them and that someone unknown to her must have remotely accessed her computer, cut and pasted the words she wrote, changed them to add further information and then posted the words on her behalf. She also denied that the post was made by her on the day alleged that it had been made.

Against this five witnesses gave testimony that they saw the post on Facebook on the day it was alleged to have been made. In a defence and in statements to the court, the defendant had also made prior inconsistent statements that led the court to conclude that the post had actually been made by the defendant. No evidence

was led in the case by either party to explain how someone else could have remotely accessed the defendant's computer and made the posts that the defendant asserted she did not make.

Showing that the post contains information only one person would know can help to authenticate the author of a post. In 2012, in the case of *Tienda v State*,[4] the Texan Court of Criminal Appeals made findings on the provenance of pages from a MySpace account. The court found that the pages belonged to the appellant because they had photographs of the appellant showing distinctive features, information about the alleged victim of the appellant, references to the appellant's gang and messages referring to an ankle monitor worn by the appellant.

Leading evidence that the post was part of an exchange of posts to circumstantially prove the provenance of a post is also possible. In 2014 in the South Australian case of *R v Usher*,[5] it was alleged that the provenance of a post could not be proven. In that case the timing of correspondence fitted the chronology of a complaint concerning an alleged rape and that was considered instructive as to the provenance of the post.

## Fairness of using social media confessions

Assuming the confession can be authenticated, the next issue to arise is whether the confession on social media is actually admissible. This is a matter for the court to decide and it is commonly the subject of a pre-trial hearing.

In the High Court of Australia case of *Tofilau v R*,[6] Gummow and Hayne JJ at [28] held that:

> There are three separate, but overlapping, inquiries that may have to be made in deciding whether evidence of an out of court confessional statement is admissible. First, there is the question, commonly described as a question of "voluntariness" presented when the confession in issue is made to someone identified as a "person in authority". Secondly, there may be the consideration of exclusion of evidence of the confession based upon notions of "basal voluntariness". Finally, there is the discretion to exclude evidence of the confession for reasons of fairness, reliability, probative value or public policy.

Their joint judgment in *Tofilau* held at [68] that:

> The chief focus for the discretionary questions that arise remains upon the fairness of using the accused person's out of court statement, rather than upon any purpose of disciplining police or controlling investigative methods.

The District Court of Queensland had reason to consider these principles in 2013 in light of confessions made on a Facebook account in the case of *R v Hasanov*.[7] In that case, the defendant, a foreign student studying in Australia with the support of a government scholarship, was charged with the indictable offence of rape of a fellow student. The defendant had been interviewed by police about the alleged rape and then afterwards there had been an exchange of messages on Facebook between the complainant and the defendant.

The defendant was alleged to have made the following post:[8]

> I am really sorry. I apologise for that night. But I ask you to think before acting. We both adult. We both were drunk. I did not mean to do anything that make you uncomfortable. If you don't want to see me again it is ok. But please understand me, you have always been respected person for me. If you want tell me your place I can come and solve the problem. I have also sister and believe me I can understand you never wanted to behave you disrespected.

The complainant then posted that she was not going to the police but wanted the defendant to admit what he did and apologise. In response, the defendant replied with a post that materially stated:

> "I am sorry, I apologise for that. I did wrong …"[9]

The defendant argued that the posts should not be admitted as evidence. He argued that the complainant was a person of authority and as such induced the defendant to make the subsequent post and so the confession in that post was not made voluntarily. He also argued that the post was not a reliable confession because the defendant may have been prepared to offer the apology just to avoid the matter being taken to the police by the complainant.

The court held that the complainant could not be seen to be a person in authority and that there was no aspect of their relationship that created an imbalance of power. The court also held that the will of the defendant was not overborne by the Facebook messages.

However, the court exercised its discretion to exclude evidence of the Facebook posts of the defendant after the initial post. The judge did this because he considered that it was possible the post was made in order to avoid police involvement for the foreign student and therefore the reliability of it as a confession was questionable.

## Conclusion

Police around the world are embracing social media as a way to obtain valuable information about criminal conduct and bring perpetrators to trial.[10] The number of users of social media is now staggering. Facebook alone has over 1.49 billion users worldwide.[11] But for there to be effective use of this veritable gold mine of evidence the authorities must ensure that they comply with the long standing rules about the admissibility of confessions as evidence. As the cases cited above have demonstrated, this can be a complex task. The intricacy of the social medium in use can and often does lead to more onerous requirements to establish proof of the

confession. However, as the cases have shown, those intricacies do not make the task insurmountable and it is therefore likely that in the future social media confessions will continue to become an important form of evidence in many criminal law cases.

***Paul Venus***
*Managing Partner — Brisbane*
*Holding Redlich*
*paul.venus@holdingredlich.com*

## Footnotes

1. See, for example, Listverse, *10 Chilling Social Media Confessions to Murder,* www.listverse.com.
2. See Evidence Act 1995 (Cth), s 90.
3. *Dabrowsk v Greeuw* [2014] WADC 175.
4. Tex Crim App 2012.
5. *R v Usher* (2014) SASCF 32; (2014) 119 SASR 22; BC201402568.
6. *Tofilau v R* (2007) 231 CLR 396; [2007] HCA 39; BC200707276.
7. *R v Hasanov* [2013] QDC 342.
8. Above n 8, at [9].
9. Above n 8, at [11].
10. See for example, MashableAsia, *20 cases solved using Facebook*, www.mashable.com.
11. Statista: The Statistics Portal, www.statista.com.

# Trade mark usage, online and offline: clarifying precisely what is usage of a trade mark

***Nicholas Smith*** *BLACKSTONE CHAMBERS*

## Tips

- When a dispute arises over the first use of a trade mark, it is important to clarify:
  - — what mark is used;
  - — when it is used; and
  - — for what goods and services.
- It is not enough to simply assert an early date of first use for all the relevant goods and services as courts will go through evidence of use to determine precisely when a mark was used and for what goods or services.
- Use of a domain name can be use of a trade mark for particular goods and services but only if the underlying website is used for those goods and services. This is the case even if the website itself does not display the trade mark.

The presence of websites, a modern day necessity in almost any form of business, has added another layer of complexity to the age old question of first use of a mark. It is now possible to acquire rights in a trade mark through first use of the mark as a domain name, even if the business or the website to which the domain name resolves to does not yet use the trade mark.

## Accor Australia & New Zealand Hospitality Pty Ltd v Liv Pty Ltd[1]

A recent case in the Federal Court of Australia has helped clarify a number of issues around first adoption and use (and hence ownership) of a trade mark, including that one can use a domain name as a trade mark even if that mark is not used in the underlying website, being the website accessed by an internet user through the domain name.

While the case involved, in the words of Rangiah J "the expenditure of resources, both by the court and the parties, on this proceeding [that seemed] grossly disproportionate to the scope of the relief sought",[2] the judgment itself is a worthy treatise on these issues and the importance of careful identification of what goods and services a particular trade mark is used and when.

The case, *Accor Australia & New Zealand Hospitality Pty Ltd v Liv Pty Ltd* involved the letting of apartments at the Cairns Harbour Lights (Harbour Lights) complex in Cairns.

## Facts of the case

Cairns Harbour Lights Pty Ltd (*CHL*) was the developer of an apartment complex in Cairns. In 2009, CHL registered Harbour Lights and Cairns Harbour Lights (the CHL Marks) as trade marks for services in Class 36 being agency services for the leasing of real estate properties; commercial real estate agency services; apartment letting agency; apartment rental services; rental of apartments; rental of accommodation; and services in Class 43 being accommodation letting agency services (holiday apartments); accommodation letting agency services (hotel); hotel accommodation services; accommodation reservation services; booking services for accommodation; and hotel services.

Accor, the first applicant, owned the exclusive rights to provide on-site letting services and an exclusive licence to use the CHL Marks. Owners were free to let their apartments on a short term basis using any letting agent, but Accor was the only letting agent able to operate on site using the CHL Marks.

The third respondent purchased an apartment in the Cairns Harbour Lights in 2005 and obtained registration of the following domain names (the Domain Names):[3]

(a) cairnsharbourlights.com.au — 4 October 2006;
(b) harbourlightscairns.com.au — 4 October 2006;
(c) harbourlightscairns.com — 17 January 2007.

The third respondent then commenced operating a business in letting apartments and later sold her business to the first respondent (*Liv*).

The applicants applied to the Federal Court and sought findings that the respondents, through the use of the Domain Names and the letting business, had engaged in trade mark infringement and misleading or deceptive conduct. The respondents sought orders that the register be rectified to remove the CHL Marks on numerous grounds, but primarily on the basis that the applicants were not the owners of the CHL Marks.

## Rectification of the registrar

Section 88 of the Trade Marks Act 1995 (Cth) provides that a prescribed court may, on the application of an aggrieved person, order that the register be rectified by, inter alia, cancelling the registration of a trade mark.

The respondents sought cancellation on the basis that CHL was not the owner of the CHL Marks for various real estate and accommodation letting services because the third respondent first used the CHL Marks when her website at the Domain Names went "live" and started advertising three apartments for let. This was, according to the respondents, before the first use of the CHL Marks by the applicants hence the applicant was not the owner of the mark pursuant to s 58 of the Trade Marks Act 1995 (Cth).

The court noted that:[4]

> …where cancellation of the registration of a trade mark is sought on the ground that the person registered as the owner is not the owner, the party seeking cancellation must prove that he or she or someone else used the trade mark in Australia earlier than the registered owner did. The party seeking cancellation must establish that the earlier use was:
> (a) use of a trade mark identical or substantially identical to the trade mark sought to be registered;
> (b) use as a trade mark;
> (c) use in respect of goods or services of the same kind or class; and
> (d) at a time when there was actual trade, or an offer to trade, in the goods or services bearing the mark, or, at least, an existing intention to offer or supply the goods or services in Australia.

## CHL's attempts to show first use

It is crucial, when establishing first use of a mark, to establish that it is being used for the goods/services that it is registered for. CHL submitted evidence that its first use was in 2004, when it registered cairnsharbourlights.com.

However, prior to 2009 the website www.cairnsharbourlights was only used for the sale of apartments, not the short term lettering services for which the respondents sought cancellation of the CHL Mark.

Additionally, the applicants' evidence did not indicate that the CHL Marks were used on the applicants' website as a badge of origin, as opposed to being descriptive of the complex, which was known as the "Cairns Harbour Lights" or "Harbour Lights".

Furthermore the applicants' use of the CHL Marks in media releases, advertisements or in email addresses was not use as a trade mark in relation to the letting of apartments. In summary the court found that CHL used the CHL Marks as trade marks in relation to "commercial real estate agency services" prior to 21 January 2009 but did not use the CHL Marks as trade marks in respect of any of the other Class 36 and Class 43 services prior to that date.

## Respondents attempts to show first use

The court then considered when the respondents first used the CHL Marks. On 31 October 2006, the respondents' website www.cairnsharbourlights.com.au went live. The website advertised the apartments owned by the third respondent. The third respondent's apartment purchase settled on 29 June 2007 and her business commenced. However, the court concluded that the marks used by the third respondent on her website were "hlp harbour lights luxury apartments" with HLP in large font and stated that:[5]

> The positioning of "hlp" was such that it would be naturally read in combination with "Harbour Lights Private Apartments", rather than separately from those words. The letters "hlp" were distinctive, including because of their size, and were not a mere descriptor attached to "Harbour Lights". In my opinion, the mark "hlp Harbour Lights Private Apartments" is not substantially identical to "Harbour Lights" or "Cairns Harbour Lights".

Despite the failure of the third respondent to use the CHL Marks on her website, the court found that her use of the Domain Names, cairnsharbourlights.com.au and harbourlightscairns.com.au to host the website were use of the CHL Marks for various real estate services from 31 October 2006 onwards.

In *Mantra Group v Tailly*,[6] Reeves J said that if a domain name is linked to a website that contains advertising material that promotes goods or services in relation to which the trade mark is registered, this combination could constitute use as a trade mark.[7] In *Mantra Group v Tailly*, Tailly leased apartments in the "Circle on Cavill" complex from owners of the apartments and then sought to sub-let these apartments to holidaymakers through a large number of websites accessible at domains that were similar to, or deliberate misspellings of, "Circle on Cavill". Mantra succeeded in obtaining findings that Tailly's use of "Circle on Cavill", including as domain names infringed Mantra's trade mark registrations and that Tailly's use was not use in good faith intended to indicate the geographical location of its apartments.

Here, the court found that the third respondent's use of the Domain Names to direct potential customers to her website which advertised her services was use of the Domain Names as a trade mark as she used the Domain Names as a badge of origin to indicate a connection between her business and the services it provided.

Furthermore the court noted that:[8]

> In considering whether the domain names are substantially identical to HARBOUR LIGHTS and CAIRNS HARBOUR LIGHTS, the prefixes "www" and suffixes ".com" and ".com.au" should be disregarded. The domain names are each substantially identical to HARBOUR LIGHTS because the word "Cairns" is merely a geographical reference, not distinctive in its own right. One of the domain names is

> identical to CAIRNS HARBOUR LIGHTS when shorn of the prefix and suffix. The rearrangement of the words in the other two domain names to "harbourlightscairns" does not substantially affect their identity. Therefore, I consider that by the use of the domain names to resolve to her website, Ms Bradnam used trade marks substantially identical to HARBOUR LIGHTS and CAIRNS HARBOUR LIGHTS.

The court also found that the respondents' use of the registered business name Harbour Lights Property and Sales was use as a trade mark and was substantially identical to Harbour Lights and Cairns Harbour Lights as the words "Property Management and Sales" were purely descriptive of the services offered by "Harbour Lights".

In summary, the court found that prior to CHL's application to register the CHL Marks, neither of the applicants used those marks or any substantially identical mark as trade marks in respect of such services other than "commercial real estate agency services", but that the respondent did use trade marks substantially identical to the CHL Marks as trade marks from 31 October 2006 for letting services. Hence, CHL was not the owner of the CHL Marks in respect of the letting services provided by the respondents and could not succeed on its trade mark claim.

## Misleading or deceptive conduct

The applicants also alleged that the respondents engaged in misconduct in order to lure customers who are looking for and intending to book accommodation with Accor (either specifically, or as the on-site manager of the property) or a hotel in Cairns to websites owned and operated by the respondents. The respondents provided a short-term apartment letting service, but not services equivalent to a hotel such as on site check in.

### *Consumer confusion is not sufficient to find misleading or deceptive conduct rather it is whether the conduct itself is misleading or deceptive*

The court noted that, while there was evidence of confusion by guests, such evidence was not helpful in deciding whether the misrepresentations alleged by applicants had actually misled or deceived guests. A finding of confusion is not essential for a finding of contravention of s 18(1) of the Australian Consumer Law (ACL) as mere confusion, without the consumer being led into error and labouring under some erroneous assumption, is insufficient to show that the conduct was misleading or deceptive.

In particular the court noted that many of the applicants' claims were based on the idea that Accor is the only "official" letting agent for the Cairns Harbour Lights complex. That was not the case. Accor was the only on-site accommodation agent appointed by the bodies corporate. Apart from the right to operate on site and the right to use the registered trade marks as trade marks, it had no more rights than any other letting agent which represented any of the lot owners.

### *Misleading or deceptive conduct: representing that one is booking a hotel room when one is only providing serviced apartments without on-site management*

While most of the applicants' claims were unsuccessful, the applicants did succeed in relation to the claim that one of the respondents — Liv Pty Ltd, had represented to potential guests looking for accommodation that the guest was booking a hotel room, or was booking a room with an on-site accommodation manager. This was because, despite being a provider of serviced apartments without on-site management, Liv had advertised on various hotel websites such as HotelClub.com.

Following expert evidence, the court concluded that for accommodation to be called a "hotel", generally the minimum requirements would include on-site reception and check-in. Those services were not provided by Liv. The court found that ordinary viewers would expect the accommodation listed on websites such as HotelClub.com to be hotel accommodation unless there was an indication that it was not. Liv provided insufficient indications to that effect. Therefore, Liv's conduct in listing its accommodation on HotelClub.com represented that a guest was booking a hotel room and/or was booking a room with an on-site accommodation manager. That conduct was misleading or deceptive in contravention of s 18(1) of the ACL. Whether or not any damages arose remains a matter for further submissions.

This decision reinforces the importance of a client actually using, or intending to use, a trade mark for all the goods and services it is sought to be registered. Failure to do that leaves a client vulnerable to an application for removal in respect of a party that has used an identical mark in respect of a particular good and service before the trade mark owner has. Equally, in respect of misleading and deceptive conduct, it is important to precisely identify which representations are made by a party's conduct; as conduct as simple as advertising serviced apartments on websites that predominantly offer hotel services, without an appropriate disclaimer, may amount to misleading and deceptive conduct.

***Nicholas Smith***
*Barrister*
*Blackstone Chambers*
*smith@nicholassmith.com.au*
*www.nicholassmith.com.au*

## Footnotes

1. *Accor Australia & New Zealand Hospitality Pty Ltd v Liv Pty Ltd* (2015) 112 IPR 494; [2015] FCA 554; BC201505256.
2. Above n 1, at [2] per Rangiah J.
3. Above n 1, at [16].
4. Above n 1, at [55].
5. Above n 1, at [178].
6. *Mantra Group v Tailly* (2010) 86 IPR 19; [2010] FCA 291; BC201001870.
7. Above n 6, at [50] per Reeves J.
8. Above n 1, at [190] per Rangiah J.

# Implementation issues with Australia's new data retention laws

***Philip Catania*** *and* ***Rebecca Measday*** *CORRS CHAMBERS WESTGARTH*

## Key points:

- Australia's new data retention laws came into effect on 13 October 2015. These laws require telecommunications service providers (including internet service providers (ISPs)) to retain certain categories of data about the use of their services for a 2 year period and to make that data available to law enforcement bodies on request.
- A number of problems with the data retention scheme have become apparent during the first few weeks of operation.
- In general, there has been difficulty with industry compliance with the new data retention scheme.
- The obligation to retain data applies to a broad range of entities, including entities that do not provide telecommunications or internet access services as part of their core business.
- The new data retention laws are likely to add a layer of complexity to the privacy compliance obligations of certain entities, including small-scale ISPs and telecommunications service providers.
- Retained data must be encrypted; however, the standard for this encryption is currently unclear. This adds another layer of cost and complexity for service providers in complying with their new obligations.
- The next 18 months will reveal the overall costs of the scheme and industry's willingness, and ability, to comply. The data retention regime will be subject to formal review in 2017–18.

New laws requiring telecommunications service providers (including ISPs) to retain certain data about the use of their services came into effect on 13 October 2015.[1] The data retention laws, which have been introduced "to allow law enforcement and intelligence agencies to obtain telecommunications data in order to safeguard national security, prevent and detect crime and protect members of the public",[2] have been criticised (including by industry bodies and consumer protection groups) as being both costly to comply with and problematic from a privacy perspective.

This article considers a number of issues with the implementation of the new data retention scheme which have become apparent during the first few weeks of operation.

## Background to the new data retention laws

New Pt 5-1 to the Telecommunications (Interception and Access) Act 1979 (Cth) (TIA Act) requires telecommunication service providers to retain certain data (known as "metadata") about communications sent via their services for a minimum of 2 years and to make that data available to Australian law enforcement bodies on request. A range of penalties (including financial penalties) apply to service providers who fail to retain data in accordance with the requirements of Pt 5-1.[3]

In general, service providers are required to retain data relating to the source, destination, time, date and duration of communications sent via their services as well as subscriber account information and information about the location of equipment used to send communications.[4] Service providers are not required to retain the content of communications sent using their services.

The data retention scheme is administered by the Communications Access Coordinator (the Coordinator) in the Attorney-General's Department.

The Bill to establish the data retention scheme was tabled on 30 October 2014 by the then Minister for Communications, Malcolm Turnbull. Despite creating privacy concerns, the Bill progressed relatively quickly through Parliament, with the final Act passing with bi-partisan support on 26 March 2015.

## Industry readiness

A survey of 63 service providers conducted by the Communications Alliance prior to 13 October 2015, found that only 16% of surveyed providers considered themselves to be "ready" to retain and encrypt data in accordance with the requirements of the TIA Act.[5]

The survey also revealed that over two thirds of surveyed providers were not confident at all or only somewhat confident that they actually understood what is required of them under the data retention scheme.

In recognition that the data retention scheme imposes significant burdens on industry, the TIA Act allows

service providers to lodge data implementation plans with the Coordinator. If a service provider's implementation plan is approved, that provider will have up to 18 months (ie, until April 2017) to achieve progressive compliance with its data retention obligations, in accordance with the approved plan.

The Coordinator has confirmed that of the 229 plans submitted by service providers prior to 21 October 2015, only 79 have been processed.[6] This leaves a large number of service providers in technical breach of their data retention obligations given that the TIA Act requires services providers to be either fully compliant with the data retention scheme or have an approved data implementation plan in place by 13 October 2015. With this in mind, the Attorney-General's Department has publically stated that the current focus of its department is on "implementation rather than enforcement".[7]

## Costs of compliance

The telecommunications industry is currently unsure which (if any) of their implementation costs will be subsidised by or recoverable from the government. The federal government has pledged $131 million in assistance to partially meet the up-front capital costs of service providers under the data retention scheme however it is unclear how this funding will be allocated among providers, with grants not expected to be provided until early 2016.[8]

Industry representatives, including Internet Australia's chief executive, Laurie Patton, have expressed concerns that the proposed funding falls short of what is needed to subsidise the implementation costs for industry.[9] According to the Communications Alliance survey, 58% of providers estimated their one-off set up costs to be between $10,000 and $250,000, with 24% estimating their costs would be over $1 million.[10] Industry spokespersons have raised concerns that the overall costs of complying with the new data retention laws may make the operations of smaller service providers (particularly ISPs) commercially unviable.

## Broad scope of the new laws

The obligation to retain data under the TIA Act applies to a broad range of entities. While the TIA Act does contain a number of general exemptions from the requirement to comply with the data retention obligations, in practice these exemptions are likely to apply on a very narrow basis.

Data retention obligations apply to carriers, carriage service providers and ISPs who own or operate infrastructure in Australia that enables the provision of telecommunications services.[11] The definitions of "carriage service provider" and "ISP" under Australian telecommunications law are quite complex and are reasonably broad in scope.

The result is that the new data retention obligations under the TIA Act are likely to apply to a range of entities that may not provide telecommunications or internet access services as part of their core businesses.

For example, some Australian universities may fall within the definitions of "carriage service provider" and "ISP" as they provide telecommunications services (including internet network access) to a range of entities located on their campuses. While Parliament originally considered whether universities should be excluded from the scope of the data retention scheme, a blanket exemption was not included in the form of the scheme as ultimately passed into law.

As a result, universities who may have data retention obligations under the TIA Act must decide whether to comply with these obligations (and incur the associated expenses) or apply to the Coordinator for a formal exemption from the requirement to comply.

Other entities that provide telecommunications and internet access services as an ancillary function to their core business will also be required to consider whether they are obligated to retain data under the TIA Act and, if so, whether they need to seek an exemption.

## Complex privacy obligations

The new data retention laws are likely to add a layer of complexity to the privacy compliance obligations of certain entities.

New s 187LA of the TIA Act requires service providers to collect and retain metadata in accordance with the Privacy Act 1988 (Cth) (Privacy Act). The TIA Act deems any data that relates to:

- an individual; or
- a communication in which an individual is a party,

which is held under Pt 5–1 of the TIA Act to be "personal information," and therefore subject to the requirements of the Privacy Act.[12]

For many service providers, the requirement to comply with the Privacy Act with respect to metadata will not change the scope of their privacy compliance obligations. However, the requirement to comply with the Privacy Act in respect of metadata may create additional compliance obligations for small-scale telecommunications service providers.

Small businesses (including telecommunications service providers) with an annual turnover of $3 million or less are generally exempt from the obligation to comply with the Privacy Act. However, under the new data

retention laws, this exemption will not apply to small businesses in relation to any data that they are required to retain under the TIA Act.

This means that small-scale telecommunications providers (who have previously been exempt from compliance with the Privacy Act) will need to ensure that they have processes and procedures in place to ensure that they are able to fully comply with the Privacy Act with respect to retained metadata.

In order to ensure privacy compliance, a small-scale telecommunications service provider will now be required to, among other things:

- develop a privacy policy which sets out information about its handling of metadata;
- provide certain notifications to individuals at or around the time that metadata is collected; and
- subject to certain exceptions, provide individuals with access to the metadata that the service provider holds about them.

The additional regulatory burdens involved in complying with the Privacy Act will increase the costs of compliance with data retention laws for small-scale providers.

Importantly, under the Privacy Act, small-scale telecommunications service providers may also be liable for the misuse of any metadata which is transferred outside of Australia. This may affect the ability of small-scale providers to take advantage of less expensive data storage solutions offshore, again increasing the cost of data retention compliance.

The data retention laws also create complicated privacy scenarios for entities, such as universities, whose general handling of personal information is governed by state-based privacy legislation, such as the Privacy and Data Protection Act 2014 (Vic). As a result of new Pt 5–1 to the TIA Act, such entities will be required to comply with:

- the applicable state-based legislation with respect to their general handling of personal information; and
- the Privacy Act with respect to metadata retained in accordance with the TIA Act.

Again, this is likely to increase the costs and complexity of compliance with the data retention laws for certain entities.

## Encryption

The TIA Act requires service providers to protect the confidentiality of retained data by encrypting that data and protecting it from unauthorised interference or unauthorised access. The legislation does not specify a standard for this encryption and the Coordinator has stated that:[13]

> The choice of the most appropriate information security and encryption measures will depend upon a range of factors, including the nature and configuration of a service provider's systems and the volume and sensitivity stored in each particular system.

According to the Coordinator, service providers can meet their encryption obligations in one of two ways:[14]

- by creating a stand-alone data store that is encrypted and protected which contains the necessary metadata while leaving general operational systems unchanged; or
- by expanding operational systems to meet the required data capture and storage requirements under the TIA Act and ensuring those systems are encrypted and protected.

The uncertainty around encryption, and the requirement for providers to either implement new systems to retain data or encrypt existing operational systems adds another layer of cost and complexity for service providers in complying with their new obligations.

## Conclusion

It is clear that there are a number of implementation issues with Australia's new data retention scheme. The next 18 months will reveal the overall cost of the scheme, industry's willingness, and ability, to comply and the benefits for law enforcement. The data retention regime will be subject to formal review by the Parliamentary Joint Committee on Intelligence and Security in 2017–2018.

***Philip Catania***
*Partner*
*Corrs Chambers Westgarth*
*philip.catania@corrs.com.au*

***Rebecca Measday***
*Associate*
*Corrs Chambers Westgarth*
*rebecca.measday@corrs.com.au*

## Footnotes

1. Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015(Cth).
2. Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth), 138.
3. See s 187M of the Telecommunications (Interception and Access) Act 1979 (Cth) and Pts 31 and 31B of the Telecommunications Act 1997 (Cth).

4. See Telecommunications (Interception and Access) Act 1979 (Cth), s 187AA.
5. The results of the survey conducted by the Communications Alliance Ltd are available at www.commsalliance.com.au.
6. The Guardian *Just a third of ISP's data retention plans have been processed by government* October 2015, www.theguardian.com.
7. Attorney-General for Australia Senator the Hon George Brandis QC "The Telecommunications (Interception And Access) Amendment (Data Retention) Act 2015" media release (13 October 2015).
8. Above n 7.
9. Internet Australia "Data Retention Act - Starts Tuesday. Oh, Really!" media release (9 October 2015).
10. Above n 5.
11. Above n 1, s 187A(3).
12. Above n 4, s 187LA.
13. Communications Access Coordinator (Cth) *Data Retention: Frequently Asked Questions for industry* (Version 1.1) July 2015.
14. Above n 13.

# Cyber threats and intellectual property

***Olivia Lamberg**, **Daniel Forrest** and **Julian Lincoln** HERBERT SMITH FREEHILLS*

## Key takeaways

- The Australian Cyber Security Centre (ACSC) has released its first unclassified *Threat Report*.
- The US and China agreed not to conduct state-sponsored cyber espionage.
- Theft of businesses' intellectual property (IP) can have a catastrophic impact on the profitability and overall viability of a company.
- Organisations are reporting losses of US$500 billion globally to cyber-crime.[1]

## Introduction

Cybersecurity has garnered significant media attention in recent times due to a number of high profile hacking incidents. On 25 September 2015, the US and China took an unprecedented step to reduce tensions on this issue by officially agreeing to not conduct state-sponsored cyber theft of commercial secrets. In related news, the Australian Cyber Security Centre (ACSC) recently released its first unclassified "*Threat Report*" which draws further attention to the unrelenting cyber threat facing Australian (governmental and private sector) organisations today.

This article specifically examines cyber security from a protection of business' trade secrets and intellectual property (IP) perspective. Recent examples of IP theft both in Australia and abroad highlight the economic and reputational cost to a business which fails to adequately protect itself from cyber intrusions.

### *The ACSC Threat Report*

The ACSC was established in November 2011 as an Australian Government initiative and has the aim of ensuring that Australian networks are among the most difficult in the world to breach. The *Threat Report* provides a snap shot of the very real threat cybercrime poses to the Australian economy. The document breaks down the technological jargon to explain the various categories of cybercrime and how the threats manifest. The report also outlines the ways in which cyber adversaries breach data security and provides details of four urgent alerts issued by the ACSC in 2014.

### *Cyber-attacks and the threat to IP*

Despite a number of high profile attacks aimed at appropriating the IP of many well-known organisations, there has been little media attention directed to the theft of IP by cyber criminals. The focus to this point has largely been directed towards protection of personal information.

The ACSC draws attention to the issue from the outset of its report. There are repeated references to the vulnerability of an organisation's IP and the hackers' abilities to obtain commercially sensitive information.[2]

## Industrial espionage in the digital age

Industrial espionage has been widespread since the late 18th and early 19th centuries. Industrial espionage involves stealing trade secrets and IP for commercial benefit. For example, details of the spinning frame that transformed textile production in England were illicitly obtained by Samuel Slater, an American spy. Upon his return to the US he set up the first water-powered textile mill based on the stolen British technology.[3]

Industrial espionage campaigns aimed at appropriating mechanical and scientific innovations from Europe facilitated the US emergence as the world's industrial leader.[4] Fast-forward to 2015 and developing countries such as China are employing similar industrial espionage tactics in cyberspace.

## IP theft: the cost to business

*"Today we see pretty much any company that has valuable intellectual property or trade secrets of any kind being pilfered continually, all day long, every day, relentlessly"*[5]

— Dimitri Alpervotich, Vice President of Threat Research at McAfee

### *Trade secrets*

Many businesses gain significant commercial advantage over their competitors through the use of trade secrets, business processes and IP. The transition into the digital age has led to a world where the highest value assets are often intangible and thus easy to copy and transfer digitally over inter-connected networks. Industrial espionage has consequently taken on a new dimension and cyber-attackers are now routinely employed to steal another business' IP. These attacks can be mounted from any location across the globe, increasing companies' risk exposure. A company's most valuable secrets can now be accessed by a sophisticated hacker from their own living room.

Hacking also occurs on an industrial scale, with more and more frequent reports of highly organised (state-sponsored) hacking attacks.

### *Cost of IP theft*

The loss of competitive advantage caused by stolen technology can significantly impact share prices and in some cases the overall viability of the business. Cybercrime such as obtaining personal details of customers or employees is typically motivated by instant financial pay off, the cost of which can also be felt by a company instantly. In contrast, the impact of the theft of trade secrets often has more severe long term consequences for business.

Steven Cross, Chairman of Aon Global Risk Consulting, has repeatedly drawn shareholders' attention to the risk of IP theft. He explains that shareholders need to pay attention to the vulnerabilities facing companies when considering stock to trade in and that shareholders should strongly support spending on cyber risk mitigation.[6]

## High profile examples of cyber theft of IP

### *Operation Aurora*

In January 2010, Google commenced discussions relating to Operation Aurora. This was the name given to a concentrated series of cyber-attacks aimed at stealing source code of a wide range of US corporations in the finance, technology, media and chemical sectors. According to security specialists, prior to the hack very little attention was paid to securing source code in contrast to financial or personally identifiable data.[7] As source code is a company's virtual DNA it is extremely important to build strong perimeters around it to protect from cyber-attack.

### *Codan hack*

Codan, an Australian communications, metal detection and mining technology firm was left devastated by a Chinese cyber intrusion. In 2011, the company began to realise there was a problem when it began to receive counterfeit metal detectors stamped with the Codan logo. They discovered that a Codan employee's laptop had been hacked when he used a wi-fi network at a hotel in China. The hacker obtained the company's blueprints and sold them to a Chinese manufacturing chain who counterfeited Codan's metal detectors. As a result of the hack, Codan was forced to slash the price of its gold detectors from around $4500 to around $2500 to compete with the counterfeiters. The company's net profit reportedly fell to $9.2 million AUD in the year to 30 June 2014 from $45 million a year earlier as a result.[8]

## Current context

Governments and corporations worldwide are beginning to comprehend the extent of the cyber-threat facing their IP.

The agreement between the US and China to not conduct cyber espionage has already been purportedly acted upon. In early October 2015, US intelligence and law enforcement agencies drew up a list of Chinese hackers that they wanted China to arrest. The Chinese government acted on this request and arrested citizens accused of carrying out espionage including those accused of conducting state-sponsored hacking for the previous Chinese regime.[9] Brian Krebs, a world expert on cyber-security, has identified at least one other incident when US government cybercrime investigators convinced Chinese authorities to take such action prior to the no cyber espionage agreement.[10]

It will be interesting to see whether the US-China agreement leads to any material or any sustained decline in the number or sophistication of cyber-attacks.

## Practical guidance

The *Threat Report* highlights the importance of educating staff, and using up-to-date antivirus software. Disturbingly, at least 85% of the targeted cyber intrusions that the Australian Signals Directorate (ASD) responds to could be prevented by following the top four mitigation strategies listed in their Strategies to Mitigate Targeted Cyber Intrusions where organisations are advised to:

1) use application whitelisting to help prevent malicious software and unapproved programs from running;
2) patch applications such as Java, PDF viewers, Flash, web browsers and Microsoft Office;
3) patch operating system vulnerabilities; and
4) restrict administrative privileges to operating systems and applications based on user duties.

Clive Lines of the ACSC urges readers of the *Threat Report* to act. "If every Australian organisation read [the Threat Report] and acted to improve their security posture, we would see a far more informed and secure Australian internet presence".[11]

***Olivia Lamberg***
*Graduate*
*Herbert Smith Freehills*

***Daniel Forrest***
*Senior Associate*
*Herbert Smith Freehills*

***Julian Lincoln***
*Partner*
*Herbert Smith Freehills*

## Footnotes

1. Gluyas R "Abbott, CEOs go covert over rising cyber threats" *The Australian* 9 July 2015.
2. Australian Cyber Security Centre *Threat Report 2015* (2015).
3. Suroweicki J "Spy Vs. Spy" *The New Yorker* 9 June 2014.
4. D Ben-Atar *Trade Secrets* Yale University Press 2004.
5. Gross M J "Enter the Cyber-Dragon" *Vanity Fair News* 15 September 2011.
6. Liew R "Shareholders must get to grips with cyber risks: Aon" *Australian Financial Review* 5 October 2015.
7. The Commission on the Theft of American Intellectual Property, *The IP Commission Report,*(May 2013).
8. Staff R "Australian company left devastated by Chinese hacking, IP theft" *CRN* 25 June 2015.
9. Nakashima E and Goldman A "In a first, Chinese hackers are arrested at the behest of the US government" *The Washington Post* 9 October 2015.
10. Krebs B "Arrest of Chinese hackers Not a first for US" *Krebs on Security* 15 October 2015.
11. Above n 2.

# Rights for screen authors Writers and Directors Worldwide: Beijing 2015 Congress

***Sabiene Heindl*** *SWH LEGAL AND BUSINESS CONSULTING*

The Writers and Directors Worldwide (WDW) congressed in Beijing, China in November 2015 welcoming authors from all corners of the world including Australia to officially launch the campaign "What If Screenrights & Directors Were Fairly Remunerated?". It was the first time that WDW had met in the Asia Pacific, demonstrating its growing commitment to strengthening authors' copyright in the region.

WDW is a Council of CISAC, the International Confederation of Societies of Authors and Composers[1] which boasts 230 members from 120 countries representing 4 million creators. In short, it is the "umbrella organisation that provides a cooperation, networking and support forum for dramatic, literary and audio-visual creators in all regions of the world."[2]

This article outlines the nature of the Beijing WDW Congress and the call for authors' rights in China and beyond.

## Introduction

*"Without an original script there is no film. Without a director there is no film."*

— Gadi Oron, Director-General CISAC[3]

Described as a significant milestone for WDW, Gadi Oron, the Director-General of CISAC welcomed delegates from four continents, including the Australian directors' and writers' organizations[4] to the inaugural meeting of WDW in the Asia Pacific. China was described as having one of the world's leading screen industries, with the influence of its writers and directors going beyond Chinese borders. Audio-visual was acknowledged as a sector with massive potential in China (36.15% increase in box office revenues in 2014) that served the local market (with 3,000+ television stations) and increasingly the global market through digital distribution.

In recent years, WDW had been encouraged by Chinese Government moves to strengthen copyright laws, including the signing of the WIPO Performers' Rights Treaty in June 2012 which represented a major benchmark for the audio-visual sector. The Chinese Government were taking significant steps to amend copyright laws and adopt an approach that took into account the interests of creators. The proposed Chinese copyright amendments, discussed below, were expected to significantly improve the rights of remuneration for audio-visual creators.

## Authors' rights and collective management

CISAC's *Global Collections Report 2014* released in October 2015 showed a return to growth for 2014 with royalties increasing by 2.8% to €7.9 billion collected on behalf of creators. For audio-visual creators, the second largest repertoire, €499 million was collected in 2014 representing a 5.2% growth. However, this was dwarfed by €6.9 billion for music.[5] The reasons were due to the lack of harmonised rights (who is recognised as an author, which rights are granted to authors and can these rights be assigned?) and the structural level of collective management for the audio-visual sector.

WDW advocates for stronger rights for creators that are inalienable. Oron's view was that what is needed is an internationally harmonised, right of fair remuneration which is unassignable. Collective management is essential because it ensures strength in authors' negotiating positions, particularly against the power of producers, broadcasters and digital platforms.

In the digital sector, internationally there had been growth of 20% in 2014 for the use of online content. However, collections from digital services accounted for only 6.5% of the global royalties around the world. Described as "alarming", 99% of those come from music repertoire with less than 1% for audio-visual content.[6] The solution proposed was to enforce stronger rights and a stronger network of collection for authors.

## Fair remuneration for authors

In Beijing, Yves Nilly, President of WDW launched the joint WDW campaign "What If Screenrights & Directors Were Fairly Remunerated?" to introduce an unassignable, unwaivable right to remuneration for screenwriters and directors worldwide. It aims to be a positive campaign with zero blame, that will educate readers on

the threat to authors' livelihoods and demonstrate the contribution that authors make both culturally and economically. The campaign for authors focuses on key planks of respect and cultural diversity.

Within this context, Delyth Thomas, Vice-Chair of Directors UK asked the question "what is fair remuneration" and how did authors work it out and who determined it? Big corporates and producers had historically defined it for audio-visual creators. Directors UK recently undertook a study to determine what fair was, particularly in circumstances where a television program or film achieved global success. Directors UK currently negotiated two tiers of remuneration with its industry agreement with broadcasters incorporating up-front fees and residuals.[7] Directors UK had commissioned an independent valuation consultancy to look at the legal position, economic theory and evidence on how courts value copyright, together with comparisons in other territories. The suggested royalty rate for directors was recommended at between 3%-5%, substantially above the industry standard of 1%. The new fee negotiated on the back of this evidence for UK directors represented a 60% increase over the previous 3 year agreement.

## The copyright landscape in China

In China, the Copyright Law protects the moral rights of writers and directors; however, copyright in the film is owned by the producer of the film. The writers and directors only have the remuneration negotiated through contracts. Indeed, copyright legislation was only introduced into China in1990 and based on the common law system. However, 20 years on it was recognised that there was growing concern about authors' rights and the need for a clearer manifestation of their rights.

The key challenges for audio-visual creators in China are online infringement and lack of fair remuneration to creators.[8] The state of collective management was also described as needing reform[9] as essential for ensuring that authors were properly remunerated and the streamlining of the collection and distribution of royalties.[10] The lack of remuneration for creators is based on the fact that:

1. Audio-visual works are protected as cinematographic works and copyright is owned by the producer. Creators only receive remuneration through contractual arrangements.
2. Audio-visual creators have a substantial lack of bargaining power and therefore often agree to single limited up-front payments only without ongoing royalty income streams.

Mr Wang Ziqiang, Department for Policy and Regulation, National Copyright Administration of China discussed the draft revision for copyright that applied to films, namely as audio-visual works and the extension of the term of copyright to the life of the author plus 50 years. It will recognise that films are derivate works from novels, scripts and so on. Therefore, there will be a need to obtain permission from the authors of these works prior to making the film. Directors and writers will be given improved rights, including ownership of copyright in the films and improved moral rights. There is also a proposed article which will strengthen copyright protection in the online environment.[11] CISAC is also actively pushing for a standard industry agreement where creators enjoy the right to share a minimum percentage of royalties for secondary use.[12]

## The copyright landscape in Australia

Representatives of Australian and New Zealand authors also attended the WDW Congress. They noted that opposition to directors' copyright has been entrenched in the common law system and through years of industry practice where producers control all rights. Stephen Wallace, Chair of ASDACS commented:[13]

> Industry practice and the lack of bargaining power of Australian directors has meant that directors' rights are simply ignored. This is justified as conducive to business whereas in reality it is exploitative and a denial of rights. Producers recognise the rights of music composers, so why do they persist in denying directors their fundamental rights? Directors are authors too.

Australian screenwriters also have an uphill battle in retaining their rights and fair remuneration for the ongoing exploitation of their work, despite having copyright in the scripts they create. This is because they face rapidly evolving and complex international distribution models and often unnecessarily aggressive and unbalanced contracting practices. Unlike legal systems in much of Europe (including the United Kingdom) and South America, writers and directors in Australia do not have any economic ownership of copyright in the film itself, despite the law being clear about their equal moral rights in the work alongside the producers.

In an era when digital technologies are changing the face of creation and distribution in the screen industry worldwide, writers and directors in Australia and New Zealand argued that it was essential to have a seat at the table through an inalienable right of remuneration for the ongoing exploitation of their films through copyright ownership.

## Conclusion

> *"As I travel the world, I find it very gratifying to be exposed to the wonderful wealth of talent that is out there—especially from younger generations—and I am constantly reminded of creators' overwhelming expectation to be treated with respect and receive fair remuneration for any*

*use of their works. We creators stand behind our societies as they adapt to new market conditions, and new challenges, to further grow their collections."*

— CISAC President Jean-Michel Jarre[14]

Authors' rights will continue to feature on the worldwide stage of copyright issues, particularly with the launch of the new campaign by WDW "What If Screenrights & Directors Were Fairly Remunerated?" to introduce an unassignable, unwaivable right to remuneration for screenwriters and directors worldwide. The steps being taken by the Chinese Government to embrace copyright for authors is a welcome step in the international fight for fair remuneration for authors of screen content.

Sadly, the reality is that if remuneration rights are not set out clearly in national copyright laws then authors' rights will continue to be trampled, as is the case in Australia.

***Sabiene Heindl***
*Executive Director*
*SWH Legal and Business Consulting*
*Sabiene_Heindl@outlook.com*

## Footnotes

1. See www.cisac.org.
2. Writers & Directors Worldwide *About Us* April 2014 www-.writersanddirectorsworldwide.org.
3. Opening statement of Gadi Oron, Director-General CISAC, to the WDW Congress in Beijing on 5 November 2015.
4. See Australian Screen Directors Authorship Collecting Society Ltd (ASDACS): www.asdacs.com.au and Australian Writers' Guild Authorship Collecting Society (AWGACS): www.awg.com.au.
5. International Confederation of Societies of Authors and Composers *CISAC Global Collections Report* (2015).
6. Above n 3.
7. Based on *hours of use x residual % x directors' salary per program hour*.
8. Mr Ben Ng, Regional-Director for Asia Pacific, CISAC on 5 November 2015.
9. Mr Tang Zhaozhi, Deputy Director General, Copyright Department, National Copyright Administration of China at the WDW Congress, Beijing, 5 November 2015.
10. Professor Wang Qian, East China University of Political Science and Law at the WDW Congress, Beijing, 5 November 2015.
11. ISP liability under Article 73.
12. That is, not on the first screening, but rather subsequent uses such as exploitation on DVD, VOD and so on.
13. Statement of ASDACS at the WDW Congress, Beijing, 6 November 2015.
14. International Confederation of Societies of Authors and Composers (CISAC) "CISAC publishes new Global Collections Report" media release (27 October 2015).

# Instant, global and permanent: Twitter, publication and privacy in Australia

***Tammy Robinson*** *BANKI HADDOCK FIORA*

## Key points

- **Twitter offers an exciting platform for individuals and companies to get their message across — in 140 characters or less.**
- **Twitter should not be regarded as any different from any other public statement.**
- **Furthermore, Twitter is in writing and the combination of unqualified brevity, instantaneity and huge reach makes it extremely dangerous for the careless or thoughtless.**

Twitter is now a major micro blogging network and a growing medium for information dissemination. Ten years old next year, Twitter currently boasts 316 million monthly active users, broadcasting (and rebroadcasting or "retweeting") more than 500 million individual tweets on any given day.[1] In Australia, more than 2.9 million Twitter accounts are used for both social and business use.[2] The rise and rise of Twitter and its legal implications have been demonstrated in two recent cases. Twitter is no longer just transitory: for those who wish to pay for it, social media data company, Gnip, offers a product that allows instant and complete access to every historical public tweet.[3] This means that every tweet ever published is permanent and searchable, creating a trap for the unwary, the unprepared or the reckless.

## Scott McIntyre and the Anzac Day tweets

On Anzac Day this year, the now ex-SBS journalist, Scott McIntyre chose Twitter to voice his opinions about the commemoration of Anzac Day in a series of tweets that most will now be familiar with, including "Wonder if the poorly-read, largely white, nationalist drinkers and gamblers pause today to consider the horror that all mankind suffered." and "Remembering the summary execution, widespread rape and theft committed by these 'brave' Anzacs in Egypt, Palestine and Japan."

The following day, McIntyre's employer, SBS, terminated his employment with immediate effect because the broadcaster considered McIntyre's "highly inappropriate and disrespectful" tweets to be in breach of the organisation's code of conduct and social media policy.[4] SBS's Social Media Protocol states: "while SBS employees have the right to make public comment … in their personal capacity, it is important to ensure that SBS is not brought into disrepute".[5] The protocol also makes it clear that strict standards apply to employees who have a high public profile including sports journalists and even for those who do not have a public profile, but identify themselves as being associated with SBS, "stricter standards will apply".[6] At the time of the Anzac Day tweets, McIntyre identified himself as an SBS journalist on his Twitter account, but should his personal views expressed in the tweets result in him losing his job?

We have witnessed Twitter disrupt the distinction between employees' work and private lives, which has required employers to find a balance between private conduct and conduct which can and should be covered by a social media policy. However, Macquarie University Associate Professor Louise Thornwaite recently observed that there has been "very little consideration given to date" on whether employers' social media policies "interfered with employees' privacy and freedom of expression expectations."[7]

Whether or not there is an unfettered implied right of political expression in Australia was considered by the Federal Circuit Court (the court) in 2013 in *Banerji v Bowles (acting Secretary, Dept of Immigration and Citizenship)*.[8] The court found that there was not and dismissed an application made by an employee of the Department of Immigration and Citizenship (as it was known then) who sought a declaration that any finding that she had breached her employer's code of conduct for tweeting her political opinions would breach her implied constitutional rights.[9] In considering the interlocutory application, Neville J held that the employee's political tweets were not constitutionally protected while she remained employed by the Department and was subject to the Department code of conduct and social media guidelines.[10]

McIntyre has lodged a discrimination claim with the Fair Work Commission (FWC) under s 351 of the Fair Work Act 2009 (Cth) (Fair Work Act), which prohibits an employer from taking adverse action against an employee (for example, dismissing that employee) because of, among other things, that employee's political opinion. It will be interesting to see whether the FWC's

interpretation of the general protections in the Fair Work Act provide any protection for employees, such as McIntyre, to maintain a personal and political identity distinct from any obligation to act in accordance with their employer's interests.

## Twitter abuse

Just as Twitter provided an instant and global means for McIntyre to share his thoughts on Anzac Day, Twitter also served as the perfect platform to amplify the reaction. While some users later tweeted their criticism of SBS's decision to dismiss McIntyre, many immediately condemned his comments, including then Minister for Communications, Malcolm Turnbull who tweeted that he found McIntyre's comments "despicable".[11] Other tweets contained personal insults about McIntyre while some users promoted the use of violence against him.[12]

Twitter has recently introduced a new system for reporting harassment after facing criticism for failing to effectively address the fact that 88% of online abuse was found to occur on its site, with only a fraction of online abuse occurring on Facebook or other social media.[13] In response, Twitter released tools that allow users to mute, block and report content and other users, including introducing shared block lists so users can create and block lists of people who are harassing them and then share their list with other users.[14] By taking these steps, Twitter has had to find the balance between protecting users' freedom of speech and addressing the problem of trolling.[15]

Trolling — when an anonymous person posts inflammatory or abusive messages online with the intent of provoking or intimidating readers — is often made possible by the use of anonymous Twitter accounts. Anonymity can remove a user's sense of responsibility for the content of their tweets and creates a vehicle for careless, reckless or even abusive comments to be made very public, like in the recent example of the @RealMark Latham Twitter account, which was trolling high profile Australian women (including Australian of the year, Rosie Batty). The news website BuzzFeed successfully linked the Twitter account with Mark Latham's personal email address suggesting that the unverified account — a blue verified badge denotes an account in which Twitter has verified the authenticity of the individual — did in fact belong to the former leader of the Australian Labor Party, Mark Latham.[16]

## Lessons from the Hockey case

Another politician featured in a highly publicised Twitter-related case recently. Former Federal Treasurer, Joe Hockey, was awarded a total of $200,000 in damages after partly succeeding in defamation proceedings he brought against three Fairfax companies. The Federal Court rejected Hockey's case in respect of a number of articles published online and in print but found that two tweets (and a *Sydney Morning Herald* poster consisting of the same wording) published by *The Age* containing the words, "Treasurer For Sale" and "Treasurer Hockey For Sale" were defamatory.[17]

It was found that the content of the articles was not defamatory in the full context, which meant that Fairfax was held liable for the promotion (via Twitter) of the headlines of the articles, rather than the story itself. The three or four defamatory words used in the tweets were brief and lacked the context of the long-form stories. It is this condensed context and brevity, necessarily constrained by Twitter's 140 character limitation, which heightens the risk of defamation. Twitter's capacity to instantly disseminate information to a global audience also has the potential to increase the damages awards in defamation cases — as we saw in the *Hockey* case when the court awarded damages of $80,000 for the two defamatory tweets.

Despite the increasing number of defamation cases involving social media, the liability of social media platforms like Twitter is not settled.[18] In a paper delivered at the March 2015 NSW State Legal Conference, Judge Judith Gibson noted that the uniform defamation legislation "drafted at a time when even the internet's possibilities were only beginning to be understood, is struggling to maintain the necessary tension between freedom of speech and protection of reputation."[19]

## Conclusion

The promotion of freedom of speech may be Twitter's mission statement, but what these recent cases demonstrate is that free speech is limited by what the law permits and defamation and employment law are not the only areas of law to impact Twitter. Copyright law, for example, poses serious challenges for Twitter. In its latest *Transparency Report*, Twitter reports that it received a total of 18,490 copyright take-down notices between 1 January 2015 and 30 June 2015, representing an 11% increase since its last report.[20] Twitter abuse and harassment has also led to a number of criminal cases overseas, including in Britain, where two Twitter users were sentenced to jail in 2014 for subjecting a feminist writer to abuse on the platform.[21] The instant, global and permanent nature of Twitter raises complex legal issues that will continue to be relevant as this increasingly influential form of social media grows.

*Note: Since the author wrote this article, Scott McIntyre has abandoned his general protections application under s 351 and has been permitted to lodge an*

*unlawful termination application under s 773 for contravention of s 772(1)(f) of the Fair Work Act 2009. For further information see: Mr Scott McIntyre v Special Broadcasting Services Corporation T/A SBS Corporation* [2015] FWC 6768.

***Tammy Robinson***
*Solicitor*
*Banki Haddock Fiora*
*robinson@bhf.com.au*

## Footnotes

1. Company Facts, Twitter's website, 30 June 2015, accessed at: https://about.twitter.com/company.
2. Queensland Government Business and Industry Portal, *Who uses Twitter?,* March 2015, www.business.qld.gov.au.
3. Luckerson V "What the Library of Congress Plans to Do With All Your Tweets" *Time* 25 February 2013, accessed at: www.business.time.com.
4. Special Broadcasting Service "Statement from SBS Managing Director Michael Ebeid and Director, Sport Ken Shipp" media release (26 April 2015).
5. "SBS Social Media Protocol" *SBS* 1 September 2011, accessed at: www.sbs.com.au.
6. Above n 5.
7. "Social media policies impinging on privacy, freedom of expression" *Workplace Express*, 29 August 2014.
8. *Banerji v Bowles (acting Secretary, Dept of Immigration and Citizenship)* [2013] FCCA 1052; BC201311780.
9. See above n 8.
10. Above n 8, at [104].
11. "SBS Presenter Scott McIntyre sacked over Anzac tweets" *The Australian* 26 April 2015.
12. Bacon W "Getting Scott McIntyre: Lest We Forget The Role of Pundits, Politicians And A Social Media Mob" *New Matilda* 6 May 2015, www newmatilda.com.
13. Edwards J "One statistic shows Twitter has a fundamental problem Facebook solved years ago" *Business Insider Australia* 19 April 2015,www.businessinsider.com.au.
14. England L "Twitter is taking another step in its attempt to deal with its trolling problem" *Business Insider Australia* 21 July 2015, www.businessinsider.com.au.
15. Above n 12.
16. Di Stefano M "Here's How We Confirmed Mark Latham Has Been Tweeting Abuse At Women" *BuzzFeed* 17 August 2015, www.buzzfeed.com.
17. *Hockey v Fairfax Media Publications Pty Limited (Hockey)* [2015] FCA 652; BC201505854.
18. Gibson JC *From McLibel to e-Libel: Recent issues and recurrent problems in defamation law"*(March 2015) pp 1 and 8, accessed at: http://glj.com.au/files/defopapergibson.pdf.
19. Above n 17, at p 2.
20. Twitter's Copyright notices *Transparency Report* (16 September 2015) accessed at: https://transparency.twitter.com/copyright-notices/2015/jan-jun.
21. Sanneh K "Censoring Twitter" *The New Yorker* 14 November 2014.

# EU Facebook decision threatens data transfers

***Brendan Scott*** *OPEN SOURCE LAW*

## Key points:

- Companies can no longer rely on the Safe Harbour scheme to export data from the EU to the US.
- Companies should be seeking "unambiguous" consent from EU citizens to the transfer of data to the US.
- The EU has set a deadline of January 2016 for the negotiation of an alternative scheme with the US, failing which coordinated enforcement actions may occur.

## Summary

A decision by the European Court of Justice in September 2015 invalidating an earlier decision of the European Commission has caused havoc for countries with an online presence in Europe, but a data presence in the United States. The ruling most likely means that companies must put in place their own measures to safeguard the privacy rights of EU citizens but, taken at its worst, could mean that companies cannot export personal data from the EU to the US.

## Legal context

The case has its origin with the EU's Data Protection Directive (95/46/EC) (the Directive). Article 25 of the Directive prohibits the transfer of data to a country unless that third country provides an "adequate level of protection" for the data. Article 26 of the Directive (discussed below) provides certain exceptions to the prohibition in Art 25. While the general law in the US does contain a variety of rights which protect the privacy of individuals, those rights do not cover all of the aspects that the Directive requires to be covered in order to meet the adequate level of protection requirement. At the time many companies wanted to have European operations which processed data in the US. The Directive would have prohibited the transport of data to the US.

In the late 90s, following the issue of the Directive, the European Commission set up a working party to examine the adequacy of privacy protections in the US. In response, the US worked towards establishing a scheme to achieve compliance with the Directive's requirements. That scheme, the "Safe Harbour" scheme found its final expression (in July 2000) in a number of principles issued by the US Federal Trade Commission (the US FTC). The Safe Harbour scheme is a voluntary scheme, albeit administered by the US FTC. US companies can elect to be covered by a number of principles and, if they do so elect, are bound to comply with them. This allowed US companies to "opt in" to a privacy protection regime without applying such a regime to all companies in the US.

Shortly after the Safe Harbour scheme was finalised, the European Commission issued a decision (Decision 2000/520/EC) finding that the scheme met the Directive's requirements. This permitted those companies covered by the scheme to export data from the EU for processing in the US. The Commission's decision stood for many years until the unveiling, by Edward Snowden in mid-2013, of the mass surveillance that was being conducted by the US government. That disclosure catalysed an existing complaint against Facebook, transforming it into a major decision.

## Initial complaints

A few years earlier, Max Schrems, an Austrian citizen, Facebook user and student studying a semester of law at the University of Santa Clara heard a guest lecture by one of Facebook's attorneys. Mr Schrems felt that the attorney's understanding of European privacy law was inadequate and decided to analyse Facebook's privacy practices as his thesis. He amassed a wealth of information critical of Facebook's treatment of personal information including a copy of Facebook's dossier on him. He released this information (redacted) online under the banner of an activist group *Europe v Facebook*.

Since Facebook is headquartered (apparently for tax reasons) in Ireland, an EU member country, it is subject to the Directive. Mr Schrems lodged complaints about Facebook to the Irish Data Protection Commissioner (DPC) which, partly as a result of Mr Schrems' complaints and partly due to the publicity at the time, conducted an investigation into Facebook's privacy practices. The DPC made some findings in late 2011 to the effect that Facebook's behaviour could be improved, but there was nothing fundamentally wrong. The report did not deal with the issue of transborder data flows in any detail, although it does observe that Facebook's data transfers were in accordance with the Safe Harbour scheme.

## Referral to the European Court of Justice

In 2013, Mr Schrems made further complaints to the DPC arguing, in light of the Snowden revelations, that the routine access to personal information by US law enforcement meant that the Safe Harbour scheme did not meet the adequacy requirements of the Directive. The DPC considered itself bound by the earlier decision of the Commission (2000/520/EC) and declined to process the complaint further. Mr Schrems applied to the Irish High Court for a review of the DPC's decision. The Irish Court referred the issue of precedence to the European Court of Justice.[1]

Around the same time, the European Commission adopted two communications to the European Parliament: *Rebuilding Trust in EU-US Data Flows* and *On the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU*.[2] These communications were critical of the surveillance carried out by US law enforcement and indicated that there was a substantial lack of compliance with the Safe Harbour requirements by Safe Harbour certified companies.

The European Court of Justice ruled that decisions, such as the Commission's Decision 2000/520/EC, do not prevent member states from investigating whether a person's rights have been infringed as a result of a transfer of data to another country if the person has put in issue the adequacy of that country's protection of personal information. It also ruled that the Commission's Decision 2000/520/EC was invalid. Therefore, Art 25 of the Directive requires EU member states to prevent the transfer of data to the US except where it falls under an exception under Art 26.

In deciding that Decision 2000/520/EC was invalid the court had regard to the manner in which surveillance was being carried out by the US (informed by the two communications listed above). In particular, while the Directive permits access to data by law enforcement authorities based on necessity, the current US practice is carried out arbitrarily and as a matter of routine. The surveillance is not judged against any objective, nor are there limiting purposes on the access to data. Individual EU citizens have no remedy available to them in the event that their privacy rights are breached (eg, they are denied access to the data held on them or their data is not rectified). This lack of remedy arises partly because, as a matter of practice, an EU citizen will have difficulty suing when an infringement of their rights occurs in the US and partly because some infringements of their rights (eg, by the US State itself) are not actionable at all.

## Consequences

The ruling invalidates a finding that the US has an adequate level of protection of private data. In theory therefore, subject to Art 26, Art 25 of the Directive requires member states to stop the transfer of data to the US. On 16 October, an EU privacy related working party[3] issued a communication stating that, given the court's decision, data transfers taking place on the basis of the Safe Harbour scheme were unlawful. The working party has set a deadline of January 2016 to find an "appropriate solution" with US authorities, failing which they foreshadow coordinated enforcement actions by data protection authorities in EU member states.

While the Safe Harbour scheme can no longer be relied upon, Art 26 provides that, even if the US does not have an adequate level of protection, a transfer can still take place if one of six exceptions is met. The most relevant of these exceptions is the first — that the data subject has given "consent unambiguously" to the proposed transfer.

Article 26 permits member states to authorise transfers for a specific person who controls data if that person can adduce evidence of safeguards protecting the privacy of individuals. Those safeguards may be contractual clauses and, indeed, there are "model contracts" available to address the protection of private data. That said, given that a key factor in the court's decision was the surveillance carried out by the US government — which companies cannot opt out of — any contractual promises given by a company will be subject to the same criticism that the Safe Harbour scheme was. Unless a political solution can be reached, any pathway to compliance with adequacy requirements will likely be undermined by the conduct of US surveillance. It is likely that reliance on the consent exception in Art 26 will emerge as the only viable basis for the export of data from the EU to the US.

***Brendan Scott***
*Open Source Law*
*www.opensourcelaw.biz*
*lists@opensourcelaw.biz*

## Footnotes

1. *Schrems v Data Protection Commissioner* [2014] IEHC 310.
2. European Commission *Rebuilding Trust in EU-US Data Flows* COM(2013) 846 final; European Commission *On the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU* COM(2013) 847 final.
3. The Art 29 Working Party on the protection of individuals comprised of a representative from the data protection authority of each EU member state.

# Duffy v Google: the latest chapter in the Google defamation story

***Eli Fisher*** *BANKI HADDOCK FIORA*

## Takeaways

- Google Inc has been found liable as a secondary publisher of defamatory content, where its search engine provides links to, and snippets of, web pages that host defamatory content.
- Google Inc has been found liable as a secondary publisher of defamatory content where its autocomplete facility or its Related Search function suggest defamatory completions to the search terms entered.
- Practitioners seeking guidance as to the notification process, when making or receiving complaints to online secondary publishers, should find assistance in Blue J's judgment.

## Introduction

On 27 October 2015, Blue J of the South Australian Supreme Court handed down his 144 page judgment in *Duffy v Google Inc*,[1] representing the latest and perhaps most significant chapter in the story about Google's liability for defamation in Australia. Many defences, particularly the statutory and common law defences of innocent dissemination are relevant to this discussion; but the plot mostly revolves around whether Google Inc can be classified as a publisher under defamation law.

## The story so far

### *UK precedents*

There have been three cases in the UK each decided by Eady J — *Bunt v Tilley*;[2] *Metropolitan International Schools Ltd v Designtechnica Corp (Metropolian International Schools)*;[3] and *Tamiz v Google Inc (Tamiz)*[4] — which have cast doubt on the ability to classify Google as a publisher capable of being held liable for defamation.

The first case, *Bunt v Tilley*, really dealt with a claim against internet service providers (ISPs) for defamation, but it formed the basis of the subsequent Eady J decisions. In *Bunt v Tilley*, his Lordship struck out the claims against the ISP defendants on the basis that they were not publishers at common law. None of the ISP defendants had been given notification of the existence of the defamatory articles. His Lordship found that the ISPs were acting in a purely passive capacity, and that "persons who truly fulfil no more than the role of a passive medium for communication cannot be characterised as publishers."[5]

In *Metropolitan International Schools*, the plaintiff sued on a defamatory web page, but also named Google Inc as a defendant, on the basis that its search results produced a snippet of the particular external website, which the plaintiff sought to enjoin. However, Eady J dismissed the plaintiff's claim against Google, and referred to his judgment in *Bunt v Tilley*, saying:[6]

> In that case, I had held as a matter of law, that an internet intermediary, if undertaking no more than the role of a passive medium of communication, cannot be characterised as a publisher at common law.

In *Tamiz*, his Lordship reached the same conclusion in respect of defamatory blogs hosted by Google, both before and after notification.[7]

### *Trkulja*[8]

In 2012, the Victorian Supreme Court gave judgment in *Trkulja v Google Inc LLC (No 5) (Trkulja)*.[9] A search of the plaintiff's name on the Google Australian website would yield search results such as the defamatory snippet "Michael Trkulja — Melbourne Crime — Underworld — Gangs", when conducting a basic word search, and, when conducting an images search, defamatory images which imputed a connection to organised crime figures.

The jury in that trial found that Google published the material resulting from each of the word and image searches of "Michael Trkulja", and that while an innocent dissemination defence may have protected Google prior to notification, Google could not avail itself of the defence following notification. Beach J dismissed Google's application challenging the jury's findings, holding that it was open to the jury to find that Google was a publisher of the defamatory material.

Beach J criticised the statements of Eady J that implied that Google's role was purely passive:[10]

> Specifically, his Lordship does not appear to have given any consideration to the fact that internet search engines, while operating in an automated fashion from the moment a request is typed into them, operate precisely as intended by those who own them and who provide their services.

Moreover, his Honour held that the statement that a person who performs no more than a passive role cannot be a publisher cuts across the principles that have formed the basis for liability in the newsagent/library cases and also where someone with power to remove a defamatory publication chooses not to do so in circumstances where an inference of consent can be drawn. This, his Honour said, does not represent the common law of Australia.

Further, his Honour rejected the notion that Google, which had itself produced the page of images that resulted when searching for the plaintiff's name, might be considered merely an "internet intermediary".[11]

The significance of this decision was that the Victorian Supreme Court had found that Google could be classified a publisher prior to notification. Even if the defence of innocent dissemination would protect such publications, Google was nevertheless a publisher.

### *Bleyer*

In *Bleyer v Google Inc (Bleyer)*,[12] a case before McCallum J in the Supreme Court of NSW, the plaintiff sued Google because the search results produced snippets derived from and hyperlinks to seven external web pages. In March 2013, Mr Bleyer asked Google Inc to remove the links, and Google removed three of the links and sought further information in relation to the other four. Mr Bleyer commenced proceedings 2 days later. McCallum J rejected the view expressed in *Trkulja*, to the extent that Beach J had considered Google to be a publisher prior to notification, and shared the view of Eady J in the three UK cases:[13]

> I would respectfully disagree with the conclusion reached by Beach J in *Trkulja* that the performance of the function of the algorithm in that circumstance is capable of establishing liability as a publisher at common law. I would adopt the English line of authority to the effect that, at least prior to notification of a complaint, … Google Inc cannot be liable as a publisher of the results produced by its search engine.

The consequences were monumental for Mr Bleyer. If Google Inc did not publish the matter complained of prior to notification, then the persons claimed by the plaintiff to have downloaded the allegedly defamatory material prior to notification could not have received the publication from Google Inc. On the plaintiff's claim, two of the three people claimed by the plaintiff to have downloaded the matters complained of did so prior to notification, and for this Google could not be held liable. For this and other reasons, McCallum J permanently stayed the proceedings on the basis that the possible benefit achievable by bringing the claim did not outweigh the costs to the court and the parties involved. This case was undoubtedly Google Inc's greatest triumph in Australian defamation litigation.

## The Duffy case

Janice Duffy met a man in New York and stayed in touch with him upon her return to Australia. She consulted with various online psychics in 2006 and 2007, from whom she sought information about the prospects of a romantic relationship with the man. The psychics made positive predictions that the two would end up together and when such did not eventuate, Dr Duffy complained to the psychics, sought a refund of her money and, among other things, created false accounts purporting to be other people, including the husband of a friend of one of the psychic's customers who had committed suicide as a result of the psychic's services.

Subsequently, in 2009, Dr Duffy became aware of numerous publications on a site called *Ripoff Report* warning psychics to be wary of her. The posts were varied, but they mostly gave rise to imputations to do with Dr Duffy stalking psychics. The web pages hosting the posts would be produced when searching the plaintiff's name on Google, and eventually, when typing "Janice Duffy" into the search bar, Google would offer "psychic stalker" as a suggested autocomplete.[14]

Dr Duffy wrote to Google seeking that the links to the defamatory material be removed. When the response was unsatisfactory, Dr Duffy commenced proceedings. There are three categories of publication that are worth considering here:

- paragraphs;
- hyperlinks; and
- autocomplete or related search suggestions.

### *Google paragraphs*

"Paragraphs" are references to each paragraph in a search results page, which comprises the title of the hyperlink, a snippet of the content at that linked web page, and the URL. Blue J had little difficulty determining that Google satisfied the physical element of the publication test:[15]

> Google was the sole operator and controller of the Google website. The paragraphs resided on Google's website. The paragraphs were communicated by Google to the user conducting a search. Google played a critical role in communicating the paragraphs to the user. The physical element of publication is present. Google did not play the passive role of a mere conduit such as an internet service provider … or a telecommunications carrier … Google played an active role in generating the paragraphs and communicating them to the user.

As to the mental element, Google intended to publish the paragraphs to the user. In addition, because Google was not a primary publisher, it was necessary that Google knew or ought to have known of the existence of the paragraphs. Thus, the mental element of publication was established on notification, if and to the extent that Google failed to remove the matters complained of after a reasonable time had elapsed (his Honour estimated 1 month, for example at [52]) after effective notification.

### *Google hyperlinks*

The issue of hyperlinks raises the question as to whether the content of the external web pages is republished by Google when users click on the links displayed by Google's search results. His Honour held that if a search of Dr Duffy's name had merely returned the URL of the matter complained of without functioning as a hyperlink and without accompanying text, it could not be said that Google was a publisher of the matter complained of. To access the material, the user would need to enter the URL, which is to say that the user would have to go and find the material him or herself. Analogously, the publisher of a database of books hosted at external libraries would not be liable for defamation if one of the books were defamatory, nor would the author of an article who includes a defamatory text in a bibliography. But, by providing the link, Google's software was found to have played an essential role in the delivery of the content of the web page to the user upon request. Accordingly, Google was found, following notification, to have been the secondary publisher of the material at external web pages.

### *Autocomplete and related search terms*

At issue here is whether Google can be considered liable as a publisher when the words "Janice Duffy psychic stalker" are generated when a user enters the search term "Janice Duffy", after Google fails to remove the suggestion within a reasonable time after notification. The same question applied to the "Related Search" suggestions. Blue J held this too to constitute a publication.

## Available defences

Google predictably relied on the defences of innocent dissemination at common law and under s 30 of the Defamation Act 2005 (NSW); but the defences cease to protect the publisher once notified, and were of no protection to Google in these circumstances.

Google attempted to rely on the common law and statutory qualified privilege defences. These both failed because the "publication was indiscriminate as to the persons to whom publication might be made and as to the purpose or interest of such persons in making the search enquiry".[16] Google attempted a novel argument that members of the public have an "interest" in being able to access information efficiently, such as through Google's service; but his Honour rejected the argument on the basis that the members of the public do not have an "interest" within the meaning of s 28(1)(a) of the Act.

Google attempted to rely on the justification defences at common law and under s 23 of the Act, but Google failed to prove that Dr Duffy stalked or persistently and obsessively harassed psychics (although Google was able to prove a more minor imputation, that she misused her government work email address). Google also failed to establish that the imputations were contextually true, which would have provided a defence under s 24 of the Act.

## Conclusion

There seems to be a growing body of authorities for the proposition that Google is a publisher, capable of being held liable for defamation once on notice. The latest judgment is particularly useful because, over its 144 pages, it provides practical details about the notification process that will be useful to practitioners representing online secondary publishers, such as search engines or social media platforms, as well as individuals defamed through, and seeking relief from, those media. It also contains the most thorough and up-to-date analysis of the relevant authorities in this area. However, this chapter of the story about Google's liability as a publisher in Australia is not yet complete. We have no indication as yet of Google's intention to appeal the judgment, and, in any event, there are remaining issues that must proceed to trial. Among them are:

- the defences of triviality and time limitation;
- the application for an extension of time; and
- the causation and quantum of damages.

We will have a far better appreciation of the result of this litigation once the issue of damages has been determined and once (if it is at all possible) any judgment against Google Inc, an American company, is enforced. McCallum J in *Bleyer* considered any such judgment to be virtually unenforceable in the US. That said, until an Australian appellate court makes a contrary determination about Google's liability as a publisher, this judgment will stand as the strongest indication in favour of that proposition.

***Eli Fisher***
*Lawyer*
*Banki Haddock Fiora*
*fisher@bhf.com.au*

## Footnotes

1. *Duffy v Google Inc* [2015] SASC 170; BC201510358.
2. *Bunt v Tilley* [2006] All ER (D) 142 (Mar) (Mar); [2006] 3 All ER 336; [2007] 1 WLR 1243; [2006] EWHC 407 (QB).
3. *Metropolitan International Schools Ltd t/as Skills Train and/or Train2Game v Designtechnica Corp t/as Digital Trends* [2009] All ER (D) 263 (Jul); [2011] 1 WLR 1743; [2009] EMLR 522; [2009] EWHC 1765 (QB).
4. *Tamiz v Google Inc* [2013] All ER (D) 163 (Feb); [2013] 1 WLR 2151; [2013] EWCA Civ 68.
5. Above n 2, at [37].
6. Above n 3, at [36].
7. Above n 4, *Tamiz* would be overturned by the Court of Appeal; but not before the *Trkulja* case was heard.
8. For more details, see E Fisher and P Knight "Google defamation trial" (2013) 15(10) *Internet Law Bulletin* p 194.
9. *Trkulja v Google Inc LLC (No 5)* [2012] VSC 533; BC201208568.
10. Above n 8, at [27].
11. Above n 8, at [29].
12. *Bleyer v Google Inc* (2014) 88 NSWLR 670; (2014) 311 ALR 529; [2014] NSWSC 897; BC201406506.
13. Above n 11, at [83].
14. For more about Google's autocomplete facility and the potential exposure Google has for defamation published via it, see E Fisher "Publication, Authorship and Technology-Generated Content" (December 2013) 31(4) *Copyright Reporter* pp 4–6.
15. Above n 1, at [204].
16. Above n 1, at [400].

# I can therefore I am entitled: the cultural justification of copyright in the digital age

***Peter Knight*** *and* ***Harry Knight*** *BANKI HADDOCK FIORA*

## Takeaway points

- Copyright is quite different from other IP (internet protocol) rights due to the cultural considerations at play.
- The Productivity Commission appears to accept uncritically the common arguments made against copyright in the context of widespread appropriation and online sharing.
- If the Commission limits its inquiry to economic considerations the outcome is unlikely to contribute to the current copyright reform debate.

The Productivity Commission released an Issues Paper in October 2015 inviting submissions on Australia's intellectual property laws.[1] The stated goal of the Commission is, among other things, to "consider whether IP arrangements strike the right balance between incentives for innovation and investment, and the interests of both individuals and businesses in accessing ideas and products".[2] The Commission proposes to evaluate copyright bundled together with other IP rights, such as patents, plant breeder's rights and trade marks.[3]

This article does not attempt to assess the economic value of copyright — we are not economists. We are concerned with the parallel debate about the cultural value of copyright — the so-called "copyright wars"[4] — and some of the common arguments made against copyright in the context of widespread appropriation and online sharing. This article will refer in particular to the online copyright infringement of professional photography.

## Copyright as Procrustean bed

There is a popular argument that copyright has failed to adapt to modern cultural practices and values.[5] As a consequence (it is said), copyright fails to balance the competing interests of creator, on the one hand, and consumers and derivative creators, on the other. In short, the argument is that copyright has become a Procrustean bed in the digital age.

The Commission appears to sympathise with this argument, making the following comparison in its Issues Paper:

> Unlike patents, copyright applies at a very low threshold to works that are merely 'original' rather than innovative or useful. And unlike patents, which offer variable degrees of protection to inventors through the provision of innovation and standard patents, copyright applies uniformly to all new works, offering a standard scope and period of protection.[6]

This is problematic for two reasons. The first is that, considering how the issue is framed, it appears to be a foregone conclusion of the Commission's inquiry that copyright is overprotected. The Commission ought to be open to more persuasion in the course of its independent research and during the public consultation process.

The second reason is that the Issues Paper appears to flag the Commission's plan to use economic rationalism in its inquiry. This is hardly surprising given the positioning of the Commission as the leading advisory body on micro-economic policy for the Federal Government. However, this approach does not take into account that copyright does not serve the economic purpose of promoting innovation and investment. The underlying purpose of copyright is, among other things, to promote creativity, which is primarily of cultural value.

This article challenges the unstated assumption of the Issues Paper that the widespread appropriation and online sharing of copyright material justifies changes to the copyright regime.

## The need to copy for art

One talking point at the recent Copyright Law and Practice Symposium 2015 was whether, and if so to what extent, artists and authors should be entitled to appropriate the works of others. The "development and convergence of information and communication technologies"[7] has been a catalyst for the appropriation and online sharing of creative content. One argument ventilated at the symposium was that the copyright regime ought to be updated to accommodate the need to copy for art.

Creative appropriation is hardly a recent phenomenon — the word "parody" derives from the ancient Greek word παρδα *(parodia)*, referring to a type of burlesque poem or song in which the words of a high-minded work were slightly altered for comic effect.[8] In context therefore mash-ups are not some cultural aberration that the copyright regime has failed to address.[9]

Creative appropriation and online sharing can be harmful to the original work. "Artist as digital cannibal", a recent article by Amalia Stone,[10] considered the transformative use of professional photography by the artist Richard Prince (of *Cariou v Prince*[11] fame) and its implications in an Australian context. Ms Stone concluded that the online percolation of derivative use can jeopardise the commercialisation of creative content and the reputation of its owner.[12]

The unauthorised use of creative content is not essential to creative appropriation and online sharing. Consider the example of the striking works of Tony Garifalakis in an exhibition on display at the National Gallery of Victoria.[13] These comprise pre-existing photographs of members of the British Royal Family, with the flesh shown in each photograph daubed over with matt black, with holes left for an eye or two, lips in some cases and some items of jewellery, and the tar-black paint dribbling. Mr Garifalakis could seek permission for his appropriation from the original owners or their intermediaries and, if permission were refused, he could use different photographs. It is possible, of course, that an appropriation artist may regard such courtesy as kow-towing to the art-as-product establishment but there would be a certain irony in this if the appropriation artist were to commercialise the resulting work.[14]

## The need to copy for consumption

In their article "Copyright cultures,"[15] Sherman Young and Steve Collins discuss the right of internet users to use and download creative content available online. "The Napster case", Young and Collins say:[16]

> … was a key case about power and control in the new digital age. It opened up arguments about the competing rights of artists, record companies and consumers over who controlled the commodity of recorded music.

They argue that such a right is well-founded in the history of copyright: in "the Encouragement of Learning"[17] and in otherwise meeting the "wider needs of society."[18]

The dictates of space do not permit Sherman and Young to explain their leap from the right to access information, which is undisputed, to the right to copy works for private use. They observe the use of copyright material for artistic purposes, especially parody, as exemplary of consumers claiming "ownership over the text." [19] Consumers however are generally not interested in artistic transformation; they simply wish to use the copyright material for their personal enjoyment — they want to listen to the song or use the picture to illustrate their blog or Facebook page.

If there is a ***need*** for a consumer to copy, this must be balanced against the need for suppliers to be paid. One can be sympathetic to the concerns of content owners whose business model depends to a significant degree on the supply of their content for private, personal and domestic non-commercial use, such as some software developers and the film and sound recording industry. Such businesses are obviously threatened by an unlimited right of private copying.

The public debate that surrounded the *Dallas Buyers Club* dispute showed to a remarkable degree an increased awareness on the part of consumers that the production of creative content can be expensive and involves risk of failure. Without revenue there will be a plethora of people who will be deprived of income — make-up artists, clapboard operators, film and sound recording crews and editors and a veritable army of other creative people whose modest livelihoods depend on receiving an income from their craft.

## The need to copy orphan works

One other common argument made against copyright in this space is that the owner may be difficult to identify.

In the 2014 report of the Australian Law Reform Commission (the ALRC), *Copyright and the Digital Economy*,[20] extrapolating from the needs of libraries and archives, the ALRC argued that anyone should be entitled to make unlimited copies for any purpose of "orphan works" unless and until the content owner is identified.

Taking again the example of professional photography, the ordinary photographer promotes and sells photographs online, and their customers often use photographs online. Often, the photographer will use reasonable copy protection measures such as watermarking. Once uploaded however the photographs are retrieved by Google searching and the more popular photographs are copied for online non-commercial use. The copy protection measures are often removed using consumer software such as Photoshop. These unprotected copies are retrieved by Google searching and the photographs percolate online. Inevitably, these photographs will be copied for online commercial use, which adversely affects the market for the photographs.

The proposed orphan works scheme would place the cost of this online percolation (and the incentive to minimise this cost) on the content owner. Given copy protection measures are routinely used, this would be an

unfair outcome, particularly where the commercial user had the means to obtain a licence in respect of the photograph or a similar photograph in advance.[21]

## The ubiquitous meme — a case study

The Awkward Penguin meme controversy is a recent example of how these common arguments are made in the context of widespread appropriation and online sharing.

The Awkward Penguin meme (right) reproduces a substantial part of the photograph taken by the professional photographer George Mobley (left). The content is owned by National Geographic and is commercialised through Getty Images.

The *Sydney Morning Herald* reported in September 2015 that Getty Images had been pursuing copyright infringement claims concerning the commercial use of the Awkward Penguin meme.[22] In response, the Awkward Penguin meme has been appropriated and shared as follows:



The original memes were infringements of the copyright subsisting in Mr Mobley's photograph. While such memes might be protected as transformative use in the US, this would not be the case in Australia.

The infringed work is a photograph of a penguin. To the eye of the ordinary consumer, the photograph has a low level of originality and should not attract the same level of copyright protection as, say, the winning portrait of the 2015 Archibald Prize.

However, the taking of this photograph would require considerable planning, skill, expense, determination and, maybe, a little serendipity.

The pre-shutter creative choices available to a professional photographer include the positioning and angling of the camera, the location and lighting of the subject, and the selection of filter, lens and exposure. The creative choices required after the photo is taken include photomontage, airbrushing, and composition. This photograph is arguably a valuable cultural contribution in its own right and Mr Mobley and other professional photographers should be encouraged to create more photographs of a similar quality to enrich our visual experience.

In contrast, the arguments made against the copyright protection of Mr Mobley's photograph bear little weight. There is no need to copy the photograph for the purpose of creative appropriation and online sharing. This is clearly illustrated by the subsequent appropriation and online sharing of the meme without the photograph being used.

There is also no need to copy the photograph for consumption because the copying is not for the purpose of accessing valuable information or for any other valuable purpose. The online percolation of this meme also has an adverse impact on the commercialisation of this photograph and similar photographs, and the photographers should not be expected to bear this cost.

## Conclusion

The copyright regime is quite different from other IP laws due to the cultural considerations at play. Our fear is that the Commission will limit its inquiry to economic considerations, and uncritically accept the common arguments made against copyright in the context of widespread appropriation and online sharing. If this fear is realised, the inquiry is unlikely to contribute to the current copyright reform debate.

***Peter Knight***
*Partner*
*Banki Haddock Fiora, Sydney*
*knight@bhf.com.au*

***Harry Knight***
*Law Graduate*
*Banki Haddock Fiora, Sydney*
*knight@bhf.com.au*

## Footnotes

1. See Australian Government Productivity Commission *Intellectual Property Arrangements Issues Paper* (October 2015), available at www.pc.gov.au (viewed 9 November 2015).
2. Above n 1, at p 1.
3. It might be asked how one would carry out a cost/benefit analysis of a basket of goods: a carrot, a tomato, an orange, an

apple, a bunch of parsley, a lamb chop, a tofu burger and a bent penny (this would be designs registration system)? All you can say is that they can all be eaten (even the bent penny, but it won't do you any good) but you don't have to!

4. See P Decherney *Hollywood's Copyright Wars: From Edison to the Internet* Columbia University Press, New York 2013.
5. See, for example, S Young and S Collins "Copyright cultures" (2015) 18(8) *Internet Law Bulletin* at p 186.
6. Above n 1, at p 19.
7. WIPO Copyright Treaty (1996).
8. *Shorter Oxford English Dictionary* Clarendon Press, Oxford 1973.
9. See, for example, *Joy Music Ltd v Sunday Pictorial Newspapers (1920) Ltd* [1960] 2 QB 60; [1960] 1 All ER 703; [1960] 2 WLR 645 (song lyrics); *Twentieth Century Fox Film Corp v Anglo-Amalgamated Film Distributors Ltd* (1965) 109 SJ 107 (artistic work in film poster) and, in Australia, *Telstra Corp Ltd v Royal & Sun Alliance Insurance Australia Ltd* (2003) 57 IPR 453; (2003) AIPC 91–903; [2003] FCA 786; BC200304197 (script for television advertisement), but compare *Williamson Music Ltd v Pearson Partnership* [1987] FSR 97 (song lyrics), *AGL Sydney Ltd v Shortland County Council* (1989) 17 IPR 99; (1990) AIPC 90–661 (script for television advertisement).
10. A Stone "Artist as digital cannibal" (2015) 18(7) *Internet Law Bulletin* at p 156.
11. *Cariou v Prince* 714 F.3d 694.
12. Above n 10, at p 157.
13. See National Gallery of Victoria, *Pleasure & Reality*, July 2015, www.ngv.vic.gov.au.
14. We are not making any comment about the works of Mr Garifalakis or his opinions.
15. Above n 5.
16. Above n 5, at p 188.
17. From the long title of the Statute of Anne Copyright Act 1709 8 Anne c 19 (GB) "An Act for the Encouragement of Learning, by Vesting the Copies of Printed Books in the Authors or Purchasers of such Copies, during the Times therein mentioned."
18. Above n 5, at p 187.
19. Above n 18. For a very thought-provoking study of the development of the "public interest" as a relevant consideration for copyright law policy, see I Alexander *Copyright Law and the Public Interest in the Nineteenth Century* Hart Publishing, Oxford and Portland, Oregon 2010.
20. Australian Law Report Commission *Copyright and the Digital Economy* Report 122, available at www.alrc.gov.au (viewed 9 November 2015).
21. The user may argue that the infringement was "innocent" and hence no damages may be claimed, by virtue of s. 115(3) of the Act. This is untenable in light of *Golden Editions Pty Ltd v Polygram Pty Ltd* (1996) 61 FCR 479; 135 ALR 638; 34 IPR 84; BC9600686 and *Milwell Pty Ltd v Olympic Amusements Pty Ltd* (1999) 85 FCR 436; 161 ALR 302; [1999] FCA 63; BC9900298. See also *Tamawood Ltd v Habitare Developments Pty Ltd (Admin Apptd) (Recs and Mgrs Apptd)* (2015) 112 IPR 439; [2015] FCAFC 65; BC201504223.
22. C Dewey "How copyright is killing your favourite memes" *Sydney Morning Herald* 13 September 2015.

**PUBLISHING EDITOR: Sarah Arkell**
**SUBSCRIPTION INCLUDES: 10 issues per year plus binder SYDNEY OFFICE: Locked Bag 2222, Chatswood Delivery Centre NSW 2067 Australia**
**For further information on this or other LexisNexis products, call Customer Relations: 1800 772 772 Monday to Friday 8.00am–6.00pm EST; email: customer.relations@lexisnexis.com.au; or visit www.lexisnexis.com.au for information on our product catalogue**.
**Editorial enquiries: Sarah.Arkell@LexisNexis.com.au**
**ISSN 1329-9735 Print Post Approved PP 244371/00049 Cite as (2015) 18(9&10) *INTLB***