CAMLA COMMUNICATIONS LAW
BULLETIN
Communications & Media Law Association Incorporated
Volume 37, No 1. March 2018

World First Inquiry Into Digital Platforms in the Media Sector

Dr Martyn Taylor (Partner), Louie Liu (Senior Associate), Emily Woolbank (Associate) of Norton Rose Fulbright consider the ACCC's new inquiry into digital platforms

The Australian Competition and Consumer Commission (**ACCC**) is conducting a 'world first' inquiry on the impact of digital platforms on competition in media and advertising markets. Public submissions are due by **3 April 2018.**

Why is the inquiry occurring?

Over the last two decades, the media and advertising sector has experienced dramatic technological change both within Australia and globally. These changes have delivered substantial benefits to consumers, but have also shifted advertising revenues away from traditional media. Concerns have been expressed that these changes have adversely impacted the quality of news and journalistic content.

As part of a Parliamentary agreement to pass significant reforms to Australia's media laws, the government agreed to ask the ACCC to conduct an 18-month inquiry into the impact of digital platforms on content creators, advertisers and consumers (**Inquiry**).

The Chairman of the ACCC, Mr Rod Sims indicated that *"the inquiry will have a particular focus on examining whether the changes affect the quality and range of news supplied to Australian consumers"* as well as *"the extent to which digital platforms curate news and journalistic content"*.

The ACCC released an Issues Paper in relation to the Inquiry on 26 February 2018, commencing formal public consultation on the issues it has been asked to consider. The ACCC is expected to produce a preliminary report by 3 December 2018, and to finalise its report by 3 June 2019.

What are digital platforms?

The Inquiry is focussed on the competitive impact of 'platform services' or 'digital platforms'. These are defined as digital search engines, social media platforms, and other digital content aggregation platforms.

Digital platforms sit on top of our 21st Century high technology ecosystem. That ecosystem includes digitalisation of information into binary data, affordable pocket supercomputers (we know as 'smartphones'), global broadband Internet communications, and sophisticated proprietary 'operating system' software that harnesses this technological power.

Platforms involve user-friendly application software (known colloquially as 'apps'). This software is often delivered at very low or no cost to consumers. The application software intermediates the delivery of content, services, and advertising using a diverse range of business models, typically facilitated by Internet-access.

Contents

CAMLA

Editors
Victoria Wark & Eli Fisher

Editorial Assistant
Imogen Yates

Printing & Distribution
BEE Printmail

Editors' Note

Welcome back, dear readers! 2018 is well underway, and as always this area has been abuzz. Where to begin? **Disney** bought the bulk of **21st Century Fox's** business, including its film and TV studios as well as its 39% stake in Sky. 22 February has come and gone, so the **mandatory data breach notification scheme** has come into effect. **Suppression orders** have been getting a lot of press, with News Corp reporting on the number of orders made per state in 2017. According to reports, Tasmania had two orders made; Queensland 10; the Northern Territory 43; South Australia and NSW, 179 and 181 respectively - and **Victoria**, 444 suppression orders. This comes as the Victorian government is reviewing the *Open Courts Act 2013*.

Geoffrey Rush is suing the **Daily Telegraph** for defamation, after it was reported that another actor complained that the actor engaged in inappropriate behaviour during a production of King Lear for the Sydney Theatre Company. **Craig McLachlan** is suing **Fairfax** and the **ABC**, after they reported on allegations that he sexually harassed former colleagues. **Seven West Media** is no longer seeking an order that **Amber Harrison** be punished for contempt.

Copyright rightsholders in the US are pleased with the result in ***TVEyes v Fox News***, which held that a service that enabled viewing whole programs in 10-minute segments was not transformative enough to be Fair Use. **Spotify** is being sued for $2 billion in copyright infringement. **Taylor Swift** has successfully shaken off a copyright claim that her song infringed 3LW's *Playas Gon' Play*, with a US judge considering that the "original" work's lyrics lacked the requisite level of creativity to be protected by copyright. In respect of such lyrics as "playas gonna play… haters gonna hate", the Judge reportedly said: "The concept of actors acting in accordance with their essential nature is not at all creative; it is banal." Judges gonna judge, we suppose. Back home on the copyright front, the Government introduced the *Copyright Amendment (Service Providers) Bill* into Parliament, has received submissions, and is due to report on 19 March 2018. The Bill proposes to extend **safe harbour**, about which proposal there is more information inside. The Government has separately announced a review of the **siteblocking** provision in s115A of the Copyright Act, with submissions due by 16 March 2018. The Australian Site Blocking Efficacy Report commissioned by the **Australian Screen Association** suggests that there has been a 53% decrease in the use of blocked sites since the siteblocking provision came into effect.

In this edition, our friends at **Norton Rose Fulbright** have written about the **ACCC's inquiry into digital platforms**, as well as on **restraints on media merger consolidation**. Speaking of Norton Rose Fulbright, we welcome (and profile) new CAMLA president **Dr Martyn Taylor**, and talk to him about what is in store for CAMLA in 2018. Privacy and data protection guru, **Peter Leonard** gives Part One of his insights into the **data breach notification scheme**. **Gilbert + Tobin** consider whether **robots are able to collude** under Australian competition law. **HWL Ebsworth** comment on the recent and the proposed changes to the *Copyright Act*, as well as the regulation of **cryptocurrencies**. And **Clayton Utz** explores how a recent Federal Court decision may have made things easier for IP rightsholders to use **preliminary discovery**.

All that makes for happy reading, but not, if you are a #younglawyer, on **14 March 2018**, when you should be at **King & Wood Mallesons** for the CAMLA **Young Lawyers Networking Event** (more details inside).

Victoria and Eli

What is the focus of the inquiry?

The focus of the Inquiry is on the impact of digital platforms on the state of competition in media and advertising services markets. Particularly, the impact of these platforms on the supply of news and journalistic content, and the implications for media content creators, advertisers and consumers.

Under the Government's Terms of Reference, the ACCC must consider:

- the extent to which platform service providers are exercising market power in commercial dealings with the creators of journalistic content and advertisers;
- the impact of platform service providers on the level of choice and quality of news and journalistic content to consumers;
- the impact of platform service providers on media and advertising markets;
- the impact of longer-term trends, including innovation and technological change, on competition in media and advertising markets; and
- the impact of information asymmetry between platform service providers, advertisers and consumers and the effect on competition in media and advertising markets.

In its Issues Paper, the ACCC has identified that it will also consider any underlying structural and behavioural issues in the relevant markets to determine whether there are competition issues. The ACCC will examine:

- whether network effects increase barriers to entry and deter effective competition from taking place;
- whether platform companies can leverage their dominance through tying or other unilateral conduct to enhance their market position, including through their ownership of personal data;
- whether transparency in media reporting and advertising has been reduced, through the use of advanced algorithms to process user data and deliver targeted content; and
- whether the advertising revenue shift away from traditional media companies could impact the creation of journalistic content and lower the quality of journalistic content.

Likely concerns for the ACCC

The Inquiry highlights the tension between the business models of traditional media (such as print media, television and radio broadcasting mediums) and the disruptive platform businesses.

Consumers are increasingly choosing to access news online, as opposed to traditional sources such as newspapers, television and radio. The ACCC has identifies that these changes in consumption habits have shifted significant proportions of advertising spend towards digital platforms. Consequently, digital platforms have become increasing important as a source of news and journalistic content for consumers, leading to concerns regarding the quality of content.

At one level, this is manifested in concerns regarding 'fake news' that became widespread during 2017. At another level, this is also manifested in concerns regarding foreign influence in electoral processes in various countries around the world. Australia's Inquiry is part of the global trend to look in greater detail at the impact of digital platform on media markets.

At the same time, the ACCC will likely closely examine the market power of digital platforms, building on work that has already been undertaken in Europe and the United States. For example:

- Digital platforms are often described as "multi-sided" in that they can generate revenue in one market (e.g. advertising) to cross-subsidise content or services in another (e.g. search).
- Digital platforms exhibit 'network effects' in that each new user add incremental value for all existing users, leading to a 'snowball' effect that is difficult for competitors to replicate.

The ACCC can be expected to consider such issues in detail over the next 18 months.

The benefits of digital platforms

As well as the concerns with digital platforms, the ACCC will consider the many benefits

From a competition law perspective, digital platforms have lowered barriers to entry for creators of content, whether it be news, journalist, or otherwise. For example, digital platforms enable a consumer to upload and share original content on a global basis at very low cost. In some cases, consumers may also receive a share of any resulting advertising revenue.

Furthermore, greater access to content via digital platforms have provided consumers with greater choice. The Internet has provided access to the entire library of knowledge and content produced by anyone, anywhere on the planet. Consumers can be significantly more selective in the content they consume, subject to the limitations of the digital platforms that they use. Bespoke content feeds are now the norm.

Historically, media was delivered through vertically-integrated platforms, such as broadcasting for free-to-air television, cable for subscription television, and print newspapers for news content. In the 21st century, any of these forms of media may be delivered via the Internet on a digital platform on virtually any Internet-enabled device. The resulting disruption is having a profound impact on the evolution of media markets, but also delivering significant value to consumers.

The questions for the ACCC, ultimately, are whether the substantial benefits delivered by digital platforms have been accompanied by detriments and, if so, whether such detriments can be appropriately addressed by competition law and policy. One does not envy the ACCC in grappling with the many nuances and complexities of this issue.

While this Inquiry is stated by the ACCC to be a 'world first', the ACCC is not alone in examining digital platforms and may consider the experiences of international regulators in other markets. For example, in 2017, a record fine of €2.42 billion was awarded by the European Commission following an investigation into alleged abuses of market dominance by a major global search engine provider.

Implications for the Inquiry

The Inquiry is being undertaken against a complex backdrop. Broader policy considerations are likely required, including the interaction of competition law, media regulation and data protection.

While the ACCC could make recommendations regarding legislative change, we think it more likely that the ACCC will use the Inquiry to better understand digital platforms and to make a series of recommendations to guide future competition policy and the ACCC's own operations.

Likely areas to watch include:

- The ACCC has a key role in reviewing mergers and acquisitions in the media sector and recently updated its Media Merger Guidelines. The findings of the Inquiry will provide an important insight into the ACCC's future approach in providing merger clearances.
- In late 2017, updates to Australia's competition laws saw changes to the misuse of market power provisions and the introduction of a new concerted practices prohibition. The ACCC may well consider whether any conduct raises issues under these provisions.
- A focus on the quality of journalistic content does not fit squarely within the remit of the ACCC. The ACCC may focus on whether any reduction in quality is due to anti-competitive behaviour or market concentration. Beyond this, the ACCC may also consider the relevance of journalistic quality for public benefit authorisations in the media sector.

Self-evidently, this Inquiry may well have global implications. This is the first time a major competition regulator has commenced an open-ended public inquiry of this nature. Consequently, we expect major stakeholders around the world will watch the developments in Australia over the coming 18 months with significant interest.

Insights Into the new Notifiable Data Breaches Scheme: Part 1

In part one of a two-part article, Peter Leonard, Principal, Data Synergies, provides some insights into the new Australian Notifiable Data Breach Scheme.

1. Introduction

A Notifiable Data Breaches scheme (**NDB scheme**) will operate in Australia from 22 February 2018.

The scheme only applies to eligible data breaches that occur on, or after, that date in Australia.

The NDB scheme requires organisations covered by the *Privacy Act 1988* (Cth) (**Privacy Act**) to notify any individuals likely to be at risk of serious harm by a data breach. This notice must take a prescribed form and must include recommendations about the steps that individuals should take in response to the data breach. The Office of the Australian Information Commissioner (**OAIC**), being the office of the Australian Privacy Commissioner (**Commissioner**), must also be notified.

Examples of a data breach include when:

- a device containing customers' personal information is lost or stolen;
- a database containing personal information is hacked; or
- personal information is mistakenly provided to the wrong person.

An 'eligible data breach' arises when the following three criteria are satisfied:

- there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds; and
- this is likely to result in serious harm to one or more individuals to whom the information relates; and
- the entity has not been able to prevent the likely risk of serious harm with remedial action.

Under the NDB scheme, if personal information is lost in circumstances where subsequent unauthorised access to or disclosure of the information is unlikely, there is no eligible data breach.[1] For example, if the personal information is remotely deleted before an unauthorised person could access the information, or if the information is encrypted to a high standard making unauthorised access or disclosure unlikely, then there is no eligible data breach.

'Serious harm' is not defined in the Privacy Act. In the context of a data breach, serious harm to an individual may include serious physical, psychological, emotional, financial, or reputational harm. Examples may include:

- identity theft;
- significant financial loss by the individual;
- threats to an individual's physical safety;
- loss of business or employment opportunities;
- humiliation, damage to reputation or relationships; and
- workplace or social bullying or marginalisation.

The likelihood of a particular harm occurring, as well as the anticipated consequences for individuals whose personal information is involved in the data breach if the harm materialises, are relevant considerations.

The following summary of the NDB scheme does not address various details such as available exceptions and exemptions. It is a general guide only. The summary extensively draws upon guidance provided by the Commissioner.[2]

2. Which entities must notify NDBs?

In general terms, agencies and organisations (entities) that are already covered by the Privacy Act must comply with the NDB scheme. More precisely, the scheme applies to entities that have an obligation under APP 11 of the Privacy Act to protect the personal information they hold.[3] Collectively known as 'APP entities', these include most Australian Government agencies, some private sector and not-for-profit organisations (Australian Privacy Principle (APP) entities, credit reporting bodies, credit providers, and tax file number (TFN) recipients), and all private health service providers.

The definition of 'APP entity' generally does not include small business operators, registered political parties, state or territory authorities, or a prescribed instrumentality of a state (s 6C). A small business operator (**SBO**) is an individual (including a sole trader), body corporate, partnership, unincorporated association, or trust that has not had an annual turnover of more than $3 million as determined applying sections 6D and 6DA of the Privacy Act.[4] Generally, SBOs do not have obligations under the APPs unless an exception applies.[5] However, if an

1 s 26WE(2)(b)(ii) of the Privacy Act.
2 As at https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme.
3 s 26WE(1)(a) of the Privacy Act.
4 s 6D of the Privacy Act.
5 s 6D(4) of the Privacy Act.

SBO falls into one of the following categories, that SBO is not exempt and must comply with the APPs, and therefore with the NDB scheme, in relation to all of the SBO's activities:

- entities that provide health services, including small businesses that provide a health service and hold people's health information. This generally includes general practitioners (GPs), pharmacists, therapists, allied health professionals, gyms and weight loss clinics, and childcare centres, among others;[6]
- entities related (through majority ownership or effective control) to an APP entity;
- entities that trade in personal information;
- credit reporting bodies;
- employee associations registered under the Fair Work (Registered Organisations) Act 2009; and
- entities that 'opt-in' to APP coverage under s 6EA of the Privacy Act.

In addition, if an SBO carries on any of the following activities it must comply with the APPs, and therefore must comply with the NDB scheme, but only in relation to personal information held by the SBO for the purpose of, or in connection with, those activities:

- providing services to the Commonwealth under a contract;
- operating a residential tenancy data base;
- reporting under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*;
- conducting a protected action ballot; and
- retention of information to comply with requirements of the mandatory data retention scheme, as per Part 5-1A of the *Telecommunications (Interception and Access) Act 1979*.

Overseas data breaches

If an APP entity discloses personal information to an overseas recipient that is not regulated as an APP entity, in line with the requirements of APP 8, then the APP entity is deemed to 'hold' the information for the purposes of the NDB scheme.[7] APP 8 says that an APP entity that discloses personal information to an overseas recipient is generally required to ensure that the recipient will comply with the APPs when handling that information. Importantly, this means that if the personal information held by the overseas recipient is subject to unauthorised access or disclosure, the APP entity is still responsible for assessing whether it is an eligible data breach under the Privacy Act, and if it is, for notifying the Commissioner and individuals at risk of serious harm.

Multiple entities

Two or more entities may hold the same personal information in a number of circumstances, including when an entity outsources the handling of personal information, is involved in a joint venture, or where it has a shared services arrangement with another entity.

If an eligible data breach involves personal information held by more than one entity, only one of the entities needs to notify the Commissioner and individuals.[8]

The NDB scheme does not specify which entity must notify, in order to allow entities flexibility in making arrangements appropriate for their business and their customers.

Entities should consider making arrangements regarding compliance with NDB scheme requirements, including notification to individuals at risk of serious harm, such as in service agreements or other relevant contractual arrangements, as a matter of course when entering into such agreements.

Other cross border issues

The Privacy Act applies to businesses that are established or incorporated in Australia (subject to the small business exemption) and Australian (federal) government agencies even when they are conducting activities outside Australia.

Accordingly, the Privacy Act has extraterritorial reach. Individuals whose personal information is protected by the Privacy Act need not be Australian citizens or Australian residents. The operation of the Privacy Act is generally tied to the status of the entity engaging in a particular act or practice, and/or the location in which an entity engages in that act or practice.

For example, where an APP entity is regulated in relation to its acts or practices outside Australia (generally being where it is a businesses established or incorporated in Australia, or an Australian (federal) government agency), those acts or practices must conform with the requirements of the Privacy Act, regardless of requirements of local law in the jurisdiction where the act or practice occurs. Generally, compliance with local law in a foreign country where the act or practice occurs, including pursuant to any law of that foreign country, does not excuse non-compliance by an APP entity with the Privacy Act. However, an act or practice outside Australia will not breach the APPs if the act or practice is both engaged in outside Australia and required by an applicable law of a foreign country.

Each entity within a corporate group is generally considered separately, although related bodies corporate are treated together for limited purposes.

The Privacy Act also regulates as an 'APP entity' a business outside Australia if that entity carries on a business in Australia and the relevant personal information is

6 https://www.oaic.gov.au/media-and-speeches/news/gps-gyms-and-childcare-centres-may-have-obligations-under-the-notifiable-data-breaches-scheme-will-your-organisation.

7 s 26WC(1) of the Privacy Act.

8 s 26WM of the Privacy Act.

collected or held by the organisation or operator in Australia or an external Territory, either before or at the time of the act or practice.[9] Accordingly, such entities are relevantly regulated only in relation to personal information collected or held by the organisation or operator in Australia or an external Territory, but not other personal information handled by such entities.

3. Making an assessment

The relevant thresholds

If an entity is aware of reasonable grounds to believe that there has been an eligible data breach, it must promptly prepare a statement about the eligible data breach for the Commissioner and notify individuals at risk of serious harm.

If an entity only has reason to suspect that there may have been a serious breach, it must move quickly to resolve that suspicion by assessing whether an eligible data breach has occurred. If, during the course of an assessment, it becomes clear that there has been an eligible breach, then the entity needs to promptly comply with the notification requirements.

The requirement for an assessment is triggered if and when an entity is aware that there are reasonable grounds to suspect that there may have been a serious breach.[10]

The Commissioner's guidance states:

> "Whether an entity is 'aware' of a suspected breach is a factual matter in each case, having regard to how a reasonable person who is properly informed would be expected to act in the circumstances. For instance, if a person responsible for compliance or personnel with appropriate seniority are aware of information that suggests a suspected breach may have occurred, an assessment should be done. An entity should not unreasonably delay an assessment of a suspected eligible breach, for instance by waiting until its CEO or Board is aware of information that would otherwise trigger reasonable suspicion of a breach within the entity.
>
> The OAIC expects entities to have practices, procedures, and systems in place to comply with their information security obligations under APP 11, enabling suspected breaches to be promptly identified, reported to relevant personnel, and assessed if necessary." [11]

Multiple entities are affected

If a data breach affects one or more other entities, and one entity has assessed the suspected breach, the other entities are not required to also assess the breach.[12] If no assessment is conducted, depending on the circumstances, each entity that holds the information may be found to be in breach of the assessment requirements. The NDB scheme does not prescribe which entity should conduct the assessment in these circumstances. Entities should establish clear arrangements where information is held jointly, so that assessments are carried out quickly and effectively.

An entity must take all reasonable steps to complete the assessment within 30 calendar days after the day the entity became aware of the grounds (or information) that caused it to suspect an eligible data breach.[13] The OAIC expects that "wherever possible entities treat 30 days as a maximum time limit for completing an assessment, and endeavour to complete the assessment in a much shorter timeframe, as the risk of serious harm to individuals often increases with time".[14]

Where an entity cannot reasonably complete an assessment within 30 days, the OAIC recommends that it should document this, so that the entity it is able to demonstrate:

- that all reasonable steps have been taken to complete the assessment within 30 days;
- what were the reasons for delay; and
- the assessment was reasonable and expeditious.[15]

4. How and when is a NDB notified?

Notice to whom?

Entities are also required to prepare a statement (a 'Notifiable Data Breach Form') and provide a copy to the Australian Information Commissioner. The statement must include the name and contact details of the entity, a description of the eligible data breach, the kind or kinds of information involved, and what steps the entity recommends that individuals at risk of serious harm take in response to the eligible data breach.[16] A form is available.[17]

Entities must also notify individuals as soon as practicable after completing the statement prepared for notifying the Commissioner.[18]

9 s 5B(3) of the Privacy Act.

10 s 26WH(1) of the Privacy Act; see also OAIC, Assessing a suspected data breach, https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/assessing-a-suspected-data-breach; OAIC, Identifying eligible data breaches, December 2017, https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/identifying-eligible-data-breaches.

11 OAIC, Assessing a suspected data breach, https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/assessing-a-suspected-data-breach.

12 s 26WJ of the Privacy Act.

13 s 26WH(2) of the Privacy Act.

14 OAIC, Assessing a suspected data breach, https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/assessing-a-suspected-data-breach.

15 Ibid.

16 s 26WK(3) of the Privacy Act.

17 https://forms.uat.business.gov.au/smartforms/landing.htm?formCode=OAIC-NDB.

18 s 26WL(3) of the Privacy Act.

Considerations of cost, time, and effort may be relevant in deciding an entity's decision about when to notify individuals. However, the Commissioner generally expects entities to expeditiously notify individuals at risk of serious harm about an eligible data breach, unless cost, time, and effort are excessively prohibitive in all the circumstances. If entities have notified individuals at risk of serious harm of the data breach before they notify the Commissioner, they do not need to notify those individuals again, so long as the individuals were notified of the contents of the statement given to the Commissioner. The scheme does not require that notification be given to the Commissioner before individuals at risk of serious harm, so if entities wish to begin notifying those individuals before, or at the same time as notifying the Commissioner, they may do so.

The NDB scheme allows three options for notifying individuals at risk of serious harm, depending on what is 'practicable' for the entity.[19]

Option 1 - Notify all individuals[20]

If it is practicable, an entity can notify all of the individuals to whom the relevant information relates.

This option may be appropriate if an entity cannot reasonably assess which particular individuals are at risk of serious harm from an eligible data breach that involves personal information about many people, but where the entity has formed the view that serious harm is likely for one or more of the individuals.

The benefits of this approach include ensuring that all individuals who may be at risk of serious harm are notified, and allowing them to consider whether they need to take any action in response to the data breach.

Option 2 - Notify only those individuals at risk of serious harm[21]

If it is practicable, an entity can notify only those individuals who are at risk of serious harm from the eligible data breach(es).

If an entity identifies that only a particular individual, or a specific subset of individuals, involved in an eligible data breach is at risk of serious harm, and can specifically identify those individuals, only those individuals need to be notified. The benefits of this targeted approach include avoiding possible notification fatigue among members of the public, and reducing administrative costs, where it is not required by the NDB scheme.

The Commissioner provides the following example:

> "An attacker installs malicious software on a retailer's website. The software allows the attacker to intercept payment card details when customers make purchases on the website. The attacker is also able to access basic account details for all customers who have an account on the website. Following a comprehensive risk assessment, the retailer considers that the individuals who made purchases during the period that the malicious software was active are at likely risk of serious harm, due to the likelihood of payment card fraud. Based on this assessment, the retailer also considers that those customers who only had basic account details accessed are not at likely risk of serious harm. The retailer is only required to notify those individuals that it considers to be at likely risk of serious harm."[22]

Option 3 - Publish notification[23]

If neither option 1 or 2 above is practicable, the entity must:

- publish a copy of the statement on its website (if the entity has one), and
- take reasonable steps to publicise the contents of the statement.

Entities must also take proactive steps to publicise the substance of the data breach (and at least the contents of the statement), to increase the likelihood that the eligible data breach will come to the attention of individuals at risk of serious harm.

An entity can notify an individual using their usual method of communicating with that particular individual.[24]

Form and content of the notification

The entity can tailor the form of its notification to individuals, which may or may not be in the form given to the Commissioner,[25] so long as long as the notification to individuals includes the content of the statement required by s 26WK, being:

- the identity and contact details of the entity;[26]
- a description of the eligible data breach that the entity has reasonable grounds to believe has happened;[27]
- the kind, or kinds, of information concerned;[28] and
- recommendations about the steps that individuals should take in response to the data breach.[29]

19 See further OAIC, Notifying individuals about an eligible data breach, December 2017, https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/notifying-individuals-about-an-eligible-data-breach.

20 s 26WL(2)(a) of the Privacy Act.

21 s 26WL(2)(b) of the Privacy Act.

22 OAIC, Notifying individuals about an eligible data breach, December 2017, https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/notifying-individuals-about-an-eligible-data-breach.

23 s 26WL(2)(c) of the Privacy Act.

24 s 26WL(4) of the Privacy Act.

25 https://forms.uat.business.gov.au/smartforms/landing.htm?formCode=OAIC-NDB.

26 s 26WK(3)(a) of the Privacy Act.

27 s 26WK(3)(b) of the Privacy Act.

28 s 26WK(3)(c) of the Privacy Act.

29 26WK(3)(d) of the Privacy Act.

The Commissioner has stated that the OAIC expects that the statement will include sufficient information about the data breach to allow affected individuals the opportunity to properly assess the possible consequences of the data breach for them, and to take protective action in response.[30] Information describing the eligible data breach may include:

- the date of the unauthorised access or disclosure;
- the date the entity detected the data breach;
- the circumstances of the data breach (such as any known causes for the unauthorised access or disclosure);
- who has obtained or is likely to have obtained access to the information; and
- relevant information about the steps the entity has taken to contain the breach.

The Commissioner provides the following example:

> "For example, to help reduce the risk of identity theft or fraud, recommendations in response to a data breach that involved individuals' Medicare numbers might include steps an individual can take to request a new Medicare card. Or in the case of a data breach that involved credit card information, putting individuals at risk of identity theft, recommendations might include that an individual contact their financial institution to change their credit card number, and also contact a credit reporting body to establish a ban period on their credit report."[31]

Multiple entities

When a data breach affects more than one entity, the entity that prepares the statement may include the identity and contact details of the other entities involved.[32] Whether an entity includes the identity and contact details of other involved entities in its statement will depend on the circumstances of the eligible data breach, and the relationship between the entities and the individuals involved. The Privacy Act does not require this information to be included on the statement, and it is open to entities to assess whether it is useful to provide this information to individuals.

The Commissioner suggests that, in general, the entity with the most direct relationship with the individuals at risk of serious harm should notify. This will allow individuals to better understand the notification, and how the eligible data breach might affect them. The Commissioner provides the following example:

> "A medical practice stores paper-based patient records with a contracted storage provider. The storage provider's premises are broken into, and the patient records stolen. While the storage provider cannot immediately determine if the stolen items included the medical practice's records, it suspects that they might have been included. Both the medical practice and the storage provider hold the records for the purpose of the Privacy Act, so both have an obligation to conduct an assessment and, if required, notify. Since the storage provider is more familiar with its facilities, the entities decide that the storage provider is best placed to conduct an assessment and determine if the records were stolen. Once the provider determines that the records were stolen, the medical practice assists the assessment by using its knowledge about the affected individuals to conclude that serious harm is likely. Although the storage provider's insurance company has agreed to cover the cost of notification, the storage provider and medical practice agree that it is most appropriate that notification come from the medical practice, as the relevant individuals do not have any pre-existing relationship with the storage provider. As such, the medical practice notifies the individuals about the incident and is reimbursed by the storage provider and its insurer for the costs of notification."[33]

The Commissioner recognises that in some instances the identity and contact details of a third party may not be relevant to an individual whose personal information is involved in an eligible data breach: for example, where the individual does not have a relationship with the other entity. In these circumstances, rather than include the identity and contact details of the third party or parties, the entity that prepares the statement may wish to describe the commercial relationship with the third party in its description of the data breach.

When must the notification be given?

Entities must prepare and give a copy of the statement to the Commissioner as soon as practicable after becoming aware of the eligible data breach.[34]

What is a 'practicable' timeframe will vary depending on the entity's circumstances, and may include considerations of the time, effort, or cost required to prepare the statement. The Commissioner has stated that the OAIC expects that once an entity becomes aware of an eligible data breach, the entity will provide a statement to the

29 26WK(3)(d) of the Privacy Act.

30 OAIC, What to include in an eligible data breach statement, December 2017, https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/what-to-include-in-an-eligible-data-breach-statement.

31 Ibid.

32 s 26WK(4) of the Privacy Act.

33 OAIC, Data breaches involving more than one organisation, December 2017, https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/data-breaches-involving-more-than-one-organisation.

34 s 26WK(2) of the Privacy Act.

Commissioner promptly, unless there are circumstances that reasonably hinder the entity's ability to do so.

5. Continuing operation of APP 11

APP 11 - *security of personal information* requires APP entities to take reasonable steps to protect personal information they hold from misuse, interference and loss, and from unauthorised access, modification or disclosure. APP 11 states:

11.1 If an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information:

a. from misuse, interference and loss; and

b. from unauthorised access, modification or disclosure.

11.2 If:

a. an APP entity holds personal information about an individual; and

b. the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity under this Schedule; and

c. the information is not contained in a Commonwealth record; and

d. the entity is not required by or under an Australian law, or a court/tribunal order, to retain the information,

the entity must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified.

Other provisions of the Privacy Act create equivalent obligations in relation to credit reporting information, credit eligibility information and tax file number information.

APP 11 has been the subject of useful guidance from the OAIC, most notably:

- OAIC, *APP Guidelines*, Chapter 11: APP 11 — Security of personal information;[35] and
- OAIC, *Guide to securing personal information*, January 2015.[36]

The NDB scheme supplements the operation of APP 11.

Before February 2018 the OAIC already received voluntary data breach notifications. The OAIC received 114 voluntary data breach notifications in the July 2016 - June 2017 financial year, a 7% increase from 107 notifications the preceding financial year.[37]

The OAIC is already responsible for mandatory data breach notifications under the *My Health Records Act* 2012 (formerly known as the Personally Controlled Electronic Health Records (**PCEHR**) scheme.

35 https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-11-app-11-security-of-personal-information.

36 https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information.

37 Office of the Australian Information Commissioner *Annual Report 2016–2017*, page 10

Editors' Note:

In part two which will be published in the next edition of this Bulletin, Peter considers the challenge posed when a data breach occurs in multiple jurisdictions and provides some insight into the regulatory approach adopted in other jurisdictions.

Peter Leonard is a data, content and technology business consultant and lawyer and principal of Data Synergies. Peter chairs the IoTAA's Data Access, Use and Privacy work stream. The IoT Alliance (www.iot.org.au) is Australia's peak IoT body, bringing together industry government and regulators to address issues affecting IoT adoption and implementation. Peter also chairs the Law Society of New South Wales' Privacy and Data Committee and the Australian Computer Society's Artificial Intelligence and Ethics Technical Committee. He serves on a number of relevant advisory boards, including of the NSW Data Analytics Centre. Peter was a founding partner of Gilbert + Tobin, now a large Australian law firm. Following his retirement as a partner in 2017 he continues to assist Gilbert + Tobin as a consultant. This paper was last revised on 12 February 2018.

Profile: Martyn Taylor

Partner at Norton Rose Fulbright and CAMLA President

CAMLA Young Lawyers representative, Calli Tsipidis, recently caught up with Martyn Taylor, to discuss his career, role as Partner of Norton Rose Fulbright in Sydney and his vision as CAMLA President for 2018.

CALLI TSIPIDIS: Congratulations on your recent appointment as the President of CAMLA! How did you initially get involved in CAMLA and what are your goals for CAMLA under your leadership?

MARTYN TAYLOR: I went to an AGM and somehow was elected to the Board. Luckily, they haven't realised yet…

Seriously, my goal is for CAMLA to remain a vibrant, interesting and successful association for the benefit of media and communications lawyers.

CAMLA is a voluntary organisation. CAMLA succeeds because we collectively make the effort to translate ideas into reality. We arrange high quality, relevant and interesting events. We produce a topical publication with outstanding content. We provide a forum for networking and sharing news. The more we each contribute, the more valuable CAMLA becomes as an association for us all.

TSIPIDIS: What would you say to encourage members of the legal profession (particularly young lawyers) to get involved in CAMLA?

TAYLOR: You have absolute control over your own destiny. Part of that is identifying opportunities and creating your own luck in life. CAMLA is one of life's opportunities. It is an opportunity to learn, to meet people, make friends, to have fun, to find out from interesting people what they think about developments in the sector – so go for it.

TSIPIDIS: Could you tell us a little bit about your role at Norton Rose Fulbright?

TAYLOR: In theory, I'm a partner in the Global Competition Team – I head the Telecoms and Media Group in the region, the Regional Trade Group and co-head the Rail Group. My areas of speciality are telecoms/media, energy, infrastructure, utilities, competition and regulatory. However, in practice, I'm a corporate and commercial lawyer who can do any transactional, advisory and contentious work in my areas of expertise.

TAYLOR: A partner wears many different hats, essentially running a business within a business. With 7 direct reports, I manage a large team. My goal is to make sure we work efficiently to meet client deadlines with high quality and commercially astute work. But also to keep everyone smiling and having plenty of fun!

TSIPIDIS: What led you to your current role and practice area?

TAYLOR: To pay my way through university, I worked full time while studying full time. My job was to assist in the project management for the construction of various power stations in the Asia-Pacific. One of those power stations was the subject of a public inquiry into CO2 emissions. I became an electricity specialist, then a utilities specialist, then became involved in the famous *Telecom v CLEAR* competition litigation. While I've been at various times a litigator, finance lawyer, M&A lawyer, and commercial lawyer, I've always remained a specialist in telecoms/media, energy, infrastructure, utilities, competition and regulatory. It is highly complex, super interesting and few people understand it.

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

TAYLOR: The most challenging aspect is managing an unbelievable workload with a sense of humour and yet finding quality time to spend with my two daughters. The most interesting aspect is solving complex problems. Law can be a four dimensional game of chess where creative moves are required, often outside the confines of the chess board. It is the thrill of finding the solution (and winning) that motivates me.

TSIPIDIS: What do you see as the biggest game changer in the telecommunications, media and technology industry?

TAYLOR: Artificial intelligence. It will be a game changer for every industry. But I'm with Elon Musk and Stephen Hawking on the risks. My smartphone is named 'HAL 9000'.

TSIPIDIS: You have been admitted as a solicitor in Australia, NZ, England and Wales – that is an incredible accomplishment. Can you tell us what your highlight was when working as a lawyer in New Zealand?

TAYLOR: Working for the ex-Prime Minister of New Zealand, Rt Hon Professor Sir Geoffrey Palmer. I was the second employee in his own start-up boutique law firm, Chen & Palmer, in 1994. We rode an incredible tsunami of the most interesting legal work in the country, often involving government lobbying. As a 23 year old, I was meeting with CEOs and cabinet ministers on a daily basis. Geoffrey was appointed a temporary judge in the International Court of Justice in the Nuclear Tests case, so I also assisted him to research his famous dissenting judgement.

TSIPIDIS: You also hold a PhD in competition and international trade law. What was your thesis and what inspired you to undertake this thesis?

TAYLOR: My thesis was that an international competition agreement should be incorporated into the World Trade Organisation. It was published in 2004 as the book "*International Competition Law: A New Dimension for the World Trade Organisation?*", which is the first footnote in Wikipedia's definition of "competition law"! My inspiration came from a paper I wrote on Japanese cultural trade barriers after winning a scholarship to represent New Zealand on a Japan Airlines scholarship to Japan. I was fascinated by the manner in which Japanese private business practices, such as the *keiretsu*, were impeding access by foreign firms into the Japanese domestic market.

TSIPIDIS: Looking back on your career and studies, what do you wish you had known about the legal profession before becoming a lawyer?

TAYLOR: I started off as an architecture student. I won the university prize in architecture, but took an unbelievable risk and switched to law. Everyone (girlfriend included) thought I was insane. That decision cost me the most beautiful girl on campus! So I'd just like to go back in time to reassure myself that it was the right decision… I've had an amazing time as a lawyer…all that emotional trauma was indeed worth it!

TSIPIDIS: In the spirit of CAMLA, media and entertainment law – if a movie were to be made of your life, who would you like to see cast as you?

TAYLOR: Tom Hanks. Not because 'life is a box of chocolates' but because I have huge respect for the manner in which he has leveraged his celebrity status to make a difference. Ditto for Leonardo DiCaprio. Ditto for Steven Spielberg as a director. They are people of integrity and substance. We need more people in the world like that.

TSIPIDIS: Finally, as a sports fanatic and working in and around sports every day, I must ask – what is your sport of choice and who is your team?

TAYLOR: I held the New Zealand title in archery in my teens. I still put that to good use each year by winning multiple, huge, stuffed teddy bears at the Royal Easter Show – my two daughters have quite a collection. Beyond that, Team New Zealand in the America's Cup (sailing). And I won't mention the All Blacks…

Calli Tsipidis is the Junior Legal Counsel at FOX SPORTS Australia and a member of the CAMLA Young Lawyers Committee.

Can Robots Collude?

Paula Gilardoni, Partner, and Andrew Low, Lawyer, at Gilbert + Tobin consider whether robots can collude.

Introduction

Businesses are increasingly using, developing and improving their ability to promptly respond to market conditions, innovate product offerings, and set prices using algorithms and artificial intelligence systems (**AI**).

Algorithm pricing systems differ from traditional more 'manual' price setting practices as they can:

- assimilate and process significant amounts of information relating to competitor prices, demand, price and availability of substitutes, and even customer personal data, almost instantaneously;
- respond almost immediately to changes in the market or competitor pricing; and
- set prices to achieve a business objective consistently across all sales.

This increased capacity to process mass amounts of information and data to execute price changes allows business to compete more effectively by responding to changes in the market quickly.

However, concerns have also been raised in relation to the use of AI pricing systems, particularly in relation to compliance with competition laws, including because:

- AI systems could facilitate, or discretely give effect to, price fixing arrangements;
- AI systems could make detection of price fixing arrangements harder; and
- the proliferation of automated AI pricing systems could result in supra competitive price levels for products and extreme forms of price discrimination between buyers.

Introduction to AI and Algorithms: What do we mean by AI and Algorithms?

Generally, AI or Artificial Intelligence refers to "intelligent" or "smart" software systems that can replicate some functions typically associated with human thought processes. There is no firm definition as to when a machine is "intelligent". Computers may be "somewhat intelligent" and others may be less so. However, today the term AI is widely used to refer to computer systems that can learn and make decisions or predictions about future behaviour (as distinct from systems that only perform repetitive tasks involving data processing that is difficult or time consuming for humans to perform).

The use of AI and algorithms is not new. Algorithms have been around since the first computers, and AI was first termed by John McCarthy in 1956. So why is it now a hot topic?

In recent times, the combination of AI, algorithms, developments in software and technology, and the proliferation of big data, has created a new wave of business processes that have relied on algorithms to increasingly make decisions that otherwise would have been performed by humans.

The OECD has broadly categorised two types of applications for algorithms:

- **Predictive analytics**: algorithms which measure the likelihood of future outcomes based on the analysis of historical data. This type of algorithm can be used to estimate demand, forecast price changes, predict customer behaviour, and other changes to the market that might affect the business.
- **Optimise business processes:** algorithms can also be used to gain a competitive advantage by reducing production and transaction cost, segmenting customers or setting optimal prices to respond to market circumstances. This is based on the algorithm's ability to process large datasets, react quickly and incur lower costs in performing functions than humans.[1]

Benefits of using algorithms

For businesses, the use of algorithms is highly compelling:

- Algorithms can perform functions that would otherwise be impossible or too time-consuming for humans to perform.
- Algorithms can make decisions and react to changes in market conditions almost instantaneously. At its simplest, if a competitor reduces its prices, an algorithm can monitor this and match that price immediately.
- Algorithms can produce efficiencies by reducing the cost of production, improving quality and resource utilisation, and streamlining business processes.
- By organising information about consumers, algorithms can help businesses better understand consumer preferences, buying patterns, reduce search costs and deliver more relevant products.

1 OECD, 'Algorithms and Collusion - Background Note by the Secretariat' (21-23 June 2017) p 9-10; accessible at https://one.oecd.org/document/DAF/COMP(2017)4/en/pdf.

2 See, Meyer v Kalonick, No. 15 Civ. 9796 (SDNY, 7 May 2016.

Consumers can also enjoy the benefits of algorithms. Price comparison websites (PCW) are a perfect example. These algorithms search and mine a large number of competing offers for the same product or service across the internet. PCWs then make it easier for consumers to compare the available offers, find the best alternative, and the best prices. In another example, an online start-up, Lemonade, uses AI to allow customers to make an insurance claims online, then verifies the claim online using a number of data sources and approves it within seconds.[3]

Despite these benefits, competition lawyers and regulators have highlighted a number of risks in relation to the use of pricing algorithms, as discussed in the next section.

Competition Law Issues and Risks: What's the issue?

Some of the risks that competition lawyers and regulators have highlighted in relation to AI systems include:

- AI systems could facilitate, or discretely give effect to, price fixing arrangements;
- AI systems could be designed to collude with other similar systems without any human interaction. Additionally, collusion could be an unintended effect, as AI systems can perform in unexpected ways (as was the case with the example referred to above in respect of *"The Making of the Fly"*). The algorithm logic made sense – price at a factor of a competitor's price. However this independent logic had an unintended consequence given the pricing corresponding algorithm);
- AI systems could result in supra competitive price levels for products; and
- The combination of automated pricing as well as big data could lead to extreme price discrimination between buyers (whereby consumers may be paying supra-competitive prices for products based on individual data used to calculate bespoke prices for each consumer).

Risks associated with collusive behaviour and price fixing are particularly important in the Australian context, more so in light of the new prohibition against concerted practices. These particular risks are examined in more detail in the sections below.

Algorithms: The Famous and the Infamous

- Uber: on 29 January 2016, an Uber rider filed a class action against Uber's CEO on the basis that Uber drivers engaged in price fixing to set supra-competitive prices through Uber's pricing algorithm. According to Uber's website:

  Uber's fares are dynamically priced. This means that the fare a rider sees is based on variables subject to change over time. These variables include (but are not limited to) the estimated time and distance of the predicted route, estimated traffic, and the number of riders and drivers using Uber at a given moment.

- Amazon marketplace: in 2011 a biology textbook *"The Making of a Fly"* was made available on Amazon for $23 million. That particular price was set through the interaction of two different sellers' programmed algorithms (see Financial Times, David J Lynch, Mehra). The first algorithm automatically set the price of the first book for 1.27x the price of the second book (which belonged to another seller). The second algorithm automatically set the price of the second book at 0.9983x the price of the first book. This led to an upward spiral in price.

- Gas stations in Rotterdam are using Denmark-based AI developer company a2I Systems A/S. Ulrik Blichfeldt, chief executive, notes his software models consumer behaviour, and learns when raising prices drives away customers and when it doesn't – leading to lower prices at time when price sensitive customers drive by (see Sam Schechner, *Why do gas station prices constantly change? Blame the algorithm, 8* May 2017, The Wall Street Journal Online). He says *"This is not a matter of stealing more money from your customer. It's about making margin on people who don't care, and giving away margin to people who do care."*

- Algorithms can also figure out what products are usually purchased together, allowing them to optimise the price of a whole shopping cart. In 2002, Andrew Pole was hired by Target to develop an algorithm which used predictive analysis to determine when a woman was entering the third trimester of pregnancy:

  "As Pole's computers crawled through the data, he was able to identify about 25 products that, when analyzed together, allowed him to assign each shopper a "pregnancy prediction" score. More important, he could also estimate her due date to within a small window, so Target could send coupons timed to very specific stages of her pregnancy."

3 OECD, p13-14.

Collusion and concerted practices under Australian laws

Under Australian competition law, prohibited conduct includes:

- entering into a contract, arrangement or understanding with a competitor with respect to cartel conduct (eg, price fixing, bid rigging, market allocation, and supply restrictions);
- "concerted practices" that have the purpose or effect of substantially lessening competition; and
- anticompetitive arrangements with the purpose or effect of substantially lessening competition.

In this framework, some form of mutuality and coordination is required in order to breach the law, and, in the usual course, some form of communication (whether direct or indirect) usually precedes any attempt at mutuality or coordination. Indeed, without any form of communication, these types of conduct would be very difficult if not impossible to engage in. Yet, in the AI world, this presents a challenge as AI systems do not necessarily "communicate" with one another in the same way as humans do.

So, how could algorithms engage in collusion or other anticompetitive conduct?

Algorithms and the facilitation of collusion

The most overt type of anticompetitive use of algorithms are ones which involve traditional forms of collusion, which are somehow aided by the use of technology.

The most obvious example of this is where algorithms are used to give effect to a pre-existing anticompetitive arrangement or understanding between competitors. This was the case in *USA v Topkins.*[4] The Department of Justice took proceedings against David Topkins. It alleged that Mr Topkins agreed with competitors to fix prices of goods sold through the Amazon marketplace by adopting an agreed upon pricing algorithm.

An anticompetitive agreement could also be facilitated if the parties to the agreement are using identical pricing software, effectively creating a "hub and spoke" cartel where the software itself (or more specifically, common knowledge about the pricing rules used by the software) becomes the de--facto "hub" used by the parties to coordinate their conduct (even in the absence of explicit or direct communications).

Generally, current competition laws in Australia could address the conduct in the examples above. However, the use of algorithms may make it harder to discover and to evidence the conduct in question. Indeed, in the second example, there could be very little if any evidence of actual interactions between competitors that could be used to prove the anticompetitive conduct.

AI and the possibility of independent "machine collusion"

Going one step further, can algorithms engage in collusion or some form of concerted conduct independent from humans? For example:

- Pricing algorithms may be developed to respond to competitor action or movement in a set manner, which over time becomes so predicable that it facilitates collusion. Say, an algorithm is set to match a competitor's price change within a particular percentage increase. Over time, the underlying rules of the algorithm become predictable and competitors have the opportunity to also respond in a similarly predictable way. For example, they may choose to only change prices in ways that will not trigger a competitive response. Competitors in that market would be able to operate with a high degree of certainty about competitive responses. Would that amount to collusion or a concerted practice?
- Pricing algorithms could also develop sufficient learning capability to assimilate, test and "understand" market responses. An algorithm may on its own, or together with other algorithms, arrive at a conclusion that "colluding" with a competing algorithm is the best way to, for example, avoid a price war or maintain profits above a certain level.

In these examples, the algorithms in question may not have been designed to engage in collusive conduct. Their objective could well be to "maximise profits", which is a perfectly legitimate business objective – however, the algorithm may discover that the best way to achieve that objective is by engaging in unilateral conduct that closely mimics "collusion". It would also be the case that there is no "communication" between the algorithms. To state the obvious, the algorithms in the example above would not be emailing each other their intentions ahead of any price movements. There is likely to be, however, a certain *pattern* and a degree of *predictability* that allows one algorithm to anticipate with sufficient accuracy what the other algorithm will do, and to adjust its responses accordingly.

Do software-driven forms of "pattern and predictability" amount to a form of communication? Or collusion? A form of concerted practice? Or is it just a machine-driven version of "conscious parallelism"?

Even if not illegal, there are concerns that the above types of algorithmic interactions may result in higher prices and less competition. This typically occurs in concentrated industries with high barriers to entry (as it is easier to establish forms of coordination), regardless of whether it is humans or software making the decisions on pricing. However, technology may also facilitate the conditions for this problem to arise by

4 Case No. 3:15-cr-00201.

making the number of competitors in the market less relevant to defeating this type of conduct (as algorithms can monitor a large number of competitors in a transparent market).

Where to next?

While there may be competition concerns relating to the potential misuse of algorithms, it remains the case that businesses should be capable of developing better technology to optimise their operations and to better compete in the modern economy. However, how can business achieve this without creating a competition law risk?

Designing Algorithms to Minimise Risk

Legal debates aside, AI will continue to develop and business will continue to seek ways to benefit from this technology.

So, what steps could be taken to try to develop pricing algorithms that will comply with competition laws?

Maintain an up-to-date record of the algorithm's design objectives

While the high level objectives of a pricing algorithm may be relatively self-evident ("optimise prices", "save costs"), it will be important to also document the ways in which that objective will be achieved and the design parameters that will be used to measure it. These records should be updated as objectives change and evolve.

It should also be noted that engaging in conduct with a purpose of "lessening competition" is likely to be problematic and could be prohibited under competition laws.

Consider the impact of the algorithm on competition

Businesses should consider whether the use of the algorithm is having an impact on competitive dynamics, in particular in regard to:

- market shares and market concentration;
- the number of competitors using the same algorithm (if any);
- price elasticity;
- barriers to entry/exit; and
- dynamic competition.

There will be many instances where the use of pricing algorithms will not have any material effect on competition. This will be the case if, for example: products are not homogenous, there are a number of different competitive factors (not just price), there are substitutes and there is the ability and incentive for competitors to "defeat" any attempt at creating supra-competitive prices.

Despite this, it will be important to test the effect at regular intervals, if any, in case the algorithm is operating in a way that is different to how it was designed.

Who else is using the same algorithm provider or software?

While bespoke or proprietary algorithms are unlikely to raise a hub and spoke issue, off-the-shelf software or the use of common algorithm providers could present some risks.

To be clear, using the same third party provider as a competitor is not in itself prohibited. In fact, it makes good sense to rely on providers that specialise in the design of algorithms for particular industries. However, to avoid any risk of unintended consequences businesses should consider:

- who else is using the same algorithm;
- whether it is, in fact, the "same" algorithm (and if so, the degree and nature of any similarities);
- what are the protections around the confidentiality of your algorithm, information, prices, and the specific algorithm used;
- retaining flexibility to adjust and vary the algorithm's operation as the need arises; and
- retaining the ability to override the algorithm in particular circumstances.

Dynamic Pricing in the Era of Big Data: An Ethical or a Competitive Problem?

New AI technologies and algorithms give businesses the ability to crunch through vast quantities of customer data. This allows businesses to set prices with a

Some Arguments Against: With Great Power Comes Great Responsibility

- *Businesses should adhere to an 'equal treatment norm'* – At the core of Krugman's conclusion about dynamic pricing is a moral objection to charging different customers different prices for the same product. This is instinctively appealing: if there is truly no difference in the underlying product, then it would seem that the person receiving the higher price has been exploited, or at least treated unfairly. Acceptance of an 'equal-treatment norm' would seem to be strongly in favour of unitary pricing as the fairest means of pricing.
- *Extreme price discrimination has the potential to defeat the fundamental purpose of certain services* – A key example is insurance, the principal objective of which is to spread risk among many members of a community. If, as a function of its programming to capture the greatest possible number of customers, an algorithm within an automated pricing system were to charge extreme prices to customers based on their exact risk factors, this would be self-defeating insofar as this social objective was concerned.
- *All pervasive algorithms may become impossible to avoid* – Another argument is that as big data becomes even more prevalent, it will become increasingly difficult and costly to avoid these systems. In this argument, customers have limited, if any, tools to protect themselves from high prices.

high degree of sophistication and to fine-tune their response to supply and demand dynamics (eg, seasonality, alternatives, switching costs, bundles, etc). To put it bluntly, algorithms allow businesses to heavily price discriminate in a bespoke way for each consumer as they can trawl through large quantities of consumers' data – such as income, purchasing habits and history, job, search history, family, address, and so on.

For some, this raises ethical questions as prices for goods are not determined by market forces – but rather, by access to customers' personal data. For others, it opens up new possibilities for increased competition.

What is 'dynamic pricing'?

Price discrimination is not a new concept. In pure price discrimination, the seller charges each customer the maximum price the customer is willing to pay. Examples include coupons, age discounts, occupational discounts, retail incentives, gender based pricing, financial aid, and ordinary haggling. Algorithms and big data however give businesses the power to "hyper" discriminate by relying upon very detailed customer information on income, spending habits, etc.

Writing in an opinion column in the New York Times in October 2000, Nobel prize winning economist Paul Krugman neatly described what he perceived as an emerging practice of 'dynamic pricing' in e-commerce:

"Dynamic pricing is a new version of an old practice: price discrimination. It uses a potential buyer's electronic fingerprint – his record of previous purchases, his address, maybe the other sites he has visited – to size up how likely he is to balk if the price is high. If the customer looks price-sensitive, he gets a bargain; if he doesn't he pays a premium."[5]

The *"old practice"* of price discrimination is common in the offline world: for example, charging different rates for male and female haircuts, or 'versioning' products so that it will be possible to charge a higher price to customers with a greater willingness to pay (for example, a novel released first in hardcover, followed later by a cheaper paperback).

However, Krugman was writing in the aftermath of the discovery of Amazon's online "price tests" – the offering of different levels of discounts to different buyers allegedly on the basis of their customer profile. Reflecting a widely held view at the time of the Amazon controversy, Krugman concluded: "dynamic pricing is undeniably unfair: some people pay more just because of who they are."

Is dynamic pricing ethical in a big data driven world?

In the years since the Amazon dynamic pricing controversy, the capacity for businesses to develop or acquire detailed customer profiles has increased. The questions and arguments as to whether these practices are ethical have not gone away either.

Are competition and consumer protection laws the answer to these ethical questions?

It can also be argued that the fact that a seller sells the same good at a lower price to a different buyer will not, by itself, be a problem. So long as data driven algorithms are not used against desperate or vulnerable individuals, or in other unconscionable circumstances, there is nothing inherently unethical in their use. There is a question, however, as to whether our consumer protection laws could address unconscionability scenarios of that nature.

It is also the case that competition itself may provide a form of protection to consumers who may be disadvantaged by dynamic pricing. So long as competition exists in a market, the fact that a company has the capacity to predict perfectly a customer's reservation price will not lead to a permanent state of price discrimination. Even where one or more firms choose to follow the original price discriminator, other rival firms or new entrants will likely be able to use the same technology to undercut those higher prices.

Technology itself may also offer consumers additional tools to fight excessive price discrimination. In the same way that algorithms can be used to determine the best price a consumer is willing to pay, algorithms can be used to find the best price at which a seller is prepared to sell. Some of those algorithms are already commonly used in some industries (eg, accommodation, petrol).

Navigating this new terrain

While there is no set roadmap for the use of these new technologies, some questions that a business may need to ask include the following:

What price discrimination strategies is the business planning to implement?

- Is there a risk that they will detrimentally impact the most vulnerable (eg, elderly customers who book flights offline paying higher prices for airfares, or less informed customers receiving smaller discounts from their electricity bills)?
- Are there regulatory concerns that may arise (eg, are there any regulatory obligations that would limit the ability to price discriminate, and what is the likelihood of a shift in the regulatory landscape in the medium term)?
- Is there enough competition in the market to allow for a healthy competitive response (eg, are there clear barriers which may prevent competitors from responding, such as advanced proprietary technology or datasets that are difficult to replicate)?
- Is the business prepared to manage any consumer backlash?

5 Paul Krugman 'Reckonings; What Price Fairness?', *New York Times*, 4 October 2000.

Copyright Act Amendments: Safe Harbour and Disability Access

Luke Dale, Partner, Eli Fisher, Senior Associate, and Jonothan Cottingham-Place, Law Clerk, at HWL Ebsworth consider some recent and proposed changes to the Copyright Act.

Summary

Safe harbour changes

The 'safe harbour' scheme, as set out in Division 2AA of Part V of the *Copyright Act 1968* (**Act**) was drafted to offer some legal protection to carriage service providers in exchange for assisting rights holders with the identification of copyright infringers. The s cheme protects carriage service providers from copyright infringements that they do not control, initiate or direct, provided they quickly remove the content upon notice.

The *Copyright Amendment (Service Providers) Bill 2017* (**Bill**), currently before the Senate, proposes to introduce several sections to the Act which extend the safe harbour scheme limitations on the scope of remedies to a broader range of 'service providers'.

Disability access

The *Copyright Amendment (Disability Access and Other Measures) Act* 2017 (**Amendment Act**) came into force on 22 December 2017, amends the Act to provide a greater level protection to those dealing with copyright works for people with certain types of disabilities.

These amendments follow Australia's ratification of the Marrakesh Treaty, and aim to improve access to published works for people who are 'blind, visually impaired and print disabled'. In summary, the Amendment Act will provide exceptions under copyright law, allowing for the legitimate reproduction of published works for visually impaired people.

Changes

Safe harbour changes

Currently, the Act provides safe harbour to "carriage service providers" in certain circumstances. As defined in the *Telecommunications Act 1997*, a carriage service provider is a person who uses a network unit to supply carriage services to the public. Under that definition, a carriage service provider most prominently includes telecommunications companies such as Optus, Telstra and TPG. The Bill intends to broaden the scope of those protected by safe harbour laws by introducing a new definition of 'service provider' under section 116ABA of the Act, which will include carriage service providers but also other categories of service providers. In particular, this will extend protection to educational institutions, libraries that either make their collection available to the public or are Parliamentary libraries, archives (including the National Archives of Australia and specified state archives), galleries, museums and key cultural institutions including specific archives and libraries that are not open to the public.

The Bill also affords safe harbour protections to organisations involved in assisting persons with a disability, including vision impairment or learning disabilities.

Disability access

The Amendment Act expands the definition of a person with a disability to include someone who has difficulty reading, viewing, hearing or comprehending copyright material in a particular form. There is also a new definition of what constitutes an organisation assisting persons with a disability, which incorporates educational institutions, or not-for-profit organisations in which the principal function is to provide assistance to people with a disability.

These amendments will broaden the scope of those able to receive access to copyright materials under the Act. This is especially important to small or not-for-profit organisations who would otherwise adopt a risk averse approach, in that it allows them to take advantage of all available resources.

What does this mean?

Safe harbour changes

If this Bill is passed, it would see safe harbour rights extended to various types of new organisations. The changes would advocate a cheaper and quicker 'notice and take down' process without court intervention for deterring copyright infringements, which may assist in protecting and promoting the rights of intellectual property owners.

The Bill will also mitigate the risks associated with providing services to the public, for example allowing for the release of unpublished documents such as reports, articles and diaries. Without safe harbour protection, this would have left service providers, such as schools, universities and libraries vulnerable to legal action, as opposed to a request to have the infringing material removed.

It is important to understand that even if the Bill is passed there will be limitations to the protections

provided, especially to Australian creators and innovators. Under the amended act, website hosting companies based in Australia will still be liable for copyright infringing content uploaded by their users and clients, leaving them with the task of ensuring all content is monitored and managed prior to use.

Disability access

The Amendment Act introduces a flexible fair dealing exception for people with a disability, and individuals or organisations assisting persons with a disability. This exception allows copyright materials to be reproduced if the purpose is for people with a disability to have access to the material. This might include braille or audio reproductions of texts, or the enhancement and enlargement of certain media, including newspapers, articles, magazines or books.

The Amendment Act also provides for a second exception, protecting organisations assisting persons with a disability, or a person acting on behalf of such an organisation. This exception allows organisations to make copies of copyright material without infringing copyright, where the purpose is to assist a person with a disability to access the material, and the material cannot be obtained in that format within a reasonable time at an ordinary commercial place. However, this exception applies only where the use of copyright material does not unreasonably impact on the commercial interests of a copyright holder. Failure to properly assess the commercial impact of a reproduction may result in penalties applying despite the protection afforded by the Amendment Act.

Comments

Generally

It is important to note that the more controversial extension of safe harbour to search engines, online platforms and cloud services, which was proposed in the Exposure Draft of the *Copyright Amendment (Disability and Other Measures) Bill 2016*, appears to have been shelved for now. Likewise, the implementation of a Fair Use regime, as proposed recently by the Australian Law Reform Commission (2014) and then the Productivity Commission (2016), has also not been advanced at this stage. Such a regime could theoretically alleviate some of the difficulties that these two reform packages are intended to address.

Safe harbour changes

Copyright owners who might previously have ignored infringements related to their intellectual property due to the time and costs associated with instituting legal proceedings might now consider filing 'notice and take down' claims with the new range of service providers.

For service providers, the Bill may afford the leeway required to extend the range of services currently provided. Universities, schools and libraries that are looking to provide greater online access to information will find themselves protected against adverse legal action as a result of intellectual property material that is published online. Libraries specifically, which provide access to online resources to the public, will be afforded a greater scope of protection, and consequently the ability to provide more information to the public. In summary, there will be a decrease in the risk of infringement for organisations that take reasonable steps to deal with copyright infringement.

Organisations should familiarise themselves with the responsibilities and obligations associated with coverage under safe harbour laws. The development of a more 'catch-all' infringement system may result in a sudden influx of notices being received by service providers. In this case, failure to act quickly and correctly may result in penalties applying.

Disability access

Organisations and individuals involved in assisting persons with a disability are now in a netter position to legitimately access, manipulate and reproduce copyright materials. It is important to note, however, that these exceptions are not without limitations. We recommend that advice should be sought in relation to copyright material prior to use, and wherever possible copyright owners should be contacted directly in advance, to ensure that the process is as fair and transparent as possible.

This article was written by **Luke Dale,** Partner, **Eli Fisher,** Senior Associate; and **Jonothan Cottingham-Place,** Law Clerk at HWL Ebsworth.

Restraints on Media Sector Consolidation
The More Prominent Role of the ACCC

Dr Martyn Taylor (Partner), Louie Liu (Senior Associate) & Stephanie Phan (Associate) of Norton Rose Fulbright, consider the ACCC's new Media Merger Guidelines

The need for reform

The regulatory framework governing the control and ownership of Australia's media was developed in an analogue media environment that was dominated by three platforms: free-to-air television, free-to-air radio and print.

While traditional media platforms remain profitable and attract significant audiences (with some exceptions), consumers are moving to new sources of video, audio and news content. Newspaper circulations, for example, have shrunk significantly in recent years and, while digital subscriptions continue to grow, they are not replacing the hard copy readership. The business of commercial broadcasting is hinged on the capacity to amass viewers for advertisers, but audiences have started to decline.

Significant concerns have been expressed that this historic framework restricts traditional media companies from optimising the scale and scope of their operations and from accessing resources, capital and management expertise available in other media sectors.

The reforms implemented in 2017 are a first step in moving Australia towards a legislative framework that is more appropriate for the modern media environment.

Changes to the media diversity rules

On 16 October 2017, the *Broadcasting Legislation Amendment (Broadcasting Reform) Act 2017 (Cth)* was enacted. Relevantly, the Act has simplified Australia's complex media cross-ownership rules by repealing the '2 out of 3' rule and '75% reach' rule. Three rules still remain, as summarised above:

Name	Rule	Status
'2 out of 3' rule	A person must not be in a position to exercise control over more than two out of the following three types of media platforms in any CRB licence area: • a commercial television broadcasting (CTVB) licence; • a commercial radio broadcasting (CRB) licence; or • an associated newspaper (essentially a significant local newspaper).	Repealed from 17 October 2017
'75% reach' rule	A person, either in their own right or as a director of one or more companies, must not be able to exercise control of CTVB licences whose combined licence area population exceeds 75% of the Australian population.	Repealed from 17 October 2017
'One-to-a-market' rule	A person, either in their own right or as a director of one or more companies, must not be able to exercise control over more than one CTVB licence in a C licence area.	Still exists
'Two-to-a-market' rule	A person, either in their own right or as a director of one or more companies, must not be able to exercise control over more than two CRB licences in the same CRB licence area.	Still exists
'4/5' rule (also known as the 'minimum voices' rule)	Under a complex points-based system, at least five independent media 'voices' must exist in a *metropolitan* CRB licence area and at least four 'voices' must exist in a *regional* CRB licence area. If there are already less than the minimum number of 'voices', then the number of 'voices' cannot be further reduced. The metropolitan CRB licence areas are the mainland state capital cities. A 'voice' is a CTVB licence, CRB licence, an associated newspaper, or a group of two or more media operations.	Still exists

The repeal of the '75% reach' rule will allow consolidation of control between metropolitan and regional broadcasters. The rule historically prevented the owners or controllers of any one of the major metropolitan commercial networks (Seven, Nine and Ten) from gaining control of (or merging with) any one of the regional commercial networks (Prime, WIN, Southern Cross Austereo). Following repeal of the rule, such consolidation could now occur, delivering cost reductions.

The repeal of the '2 out of 3' rule will allow a person that controls two regulated media platforms in a licence area to acquire control of additional regulated platforms in the same licence area. In most licence areas, no single entity controls media assets from two of the three regulated platforms so repeal of this rule may have little practical impact However, Fairfax Media is one entity that could not historically control a commercial television licence

in Sydney or Melbourne unless it divested its commercial radio or associated newspaper in the relevant licence area.

The elevated role of the ACCC

The removal of two of the statutory restrictions on media cross-ownership, means that the Australian Competition and Consumer Commission (ACCC) will now become more of a gatekeeper for media market consolidation than has historically been the case

Importantly, the ACCC has always been a gatekeeper for mergers in concentrated sectors. The merger rule in section 50 of the *Competition and Consumer Act 2010 (Cth)* applies to all sectors of the economy to protect against excessive concentration of market power. Media sector acquisitions are prohibited if they have the effect, or are likely to have the effect, of substantially lessening competition in any Australian market.

However, the relaxation of the statutory restrictions does mean that the ACCC's future role will be more prominent. The ACCC has recognised this by releasing updated *Media Merger Guidelines* (**Guidelines**) which outline the ACCC's approach to media mergers, both in traditional and new media. The Guidelines update the previous version, dating from 2006, and supplement the ACCC's standard merger guidelines.

In the Guidelines, the ACCC identifies that common areas of competitive overlap in the media sector typically involve one or more of the following activities:

- the supply of content to consumers, either directly or via a firm which acquires and aggregates content for supply to consumers;
- the supply of advertising opportunities to advertisers; and/or
- the acquisition of content from content providers.

The ACCC defines the relevant markets in light of these core activities by considering the extent of substitution, consistent with its usual approach. In doing so, the ACCC will consider substitution between modes of delivery (such as print, radio broadcasting, free-to-air television broadcasting, digital media platforms, and over-the-top video streaming) as well as the extent of convergence between those modes. The ACCC will also consider substitution between different types of content or advertising opportunities (such as sport, entertainment, and quality news content).

Within these markets, the ACCC will consider potential adverse effects arising from any reduction in competition to develop a 'theory of harm'. Consistent with the ACCC's standard merger guidelines, the ACCC will focus on unilateral effects (such as price rises, reduced service quality, and reduced incentive to innovation) and co-ordinated effects (such as greater risk of price co-ordination). It is within this general framework that the ACCC will focus on bespoke issues that tend to be more prominent in media mergers than in other mergers.

Potential ACCC concerns with media mergers

In the Guidelines, the ACCC has identified five key issues to which it may attribute greater prominence in media merger assessments. Where concerns arise, the ACCC will normally be receptive to the parties offering a remedy, usually by way of court-enforceable undertaking:

1. Competition and media diversity

The ACCC views media diversity through the prism of market concentration and competition. A merger that increases market concentration will reduce the number of 'voices', reduce choice for consumers and potentially reduce quality of content, thereby reducing media diversity. In a media context, the ACCC will be concerned not only with adverse price impacts of a merger, but also on non-price impacts, particularly any adverse impacts on the quality of content for consumers.

If a merger party were to seek formal authorisation from the ACCC of a media merger, rather than the usual informal clearance route, recent New Zealand case law also suggests that the issue of media diversity may be relevant to an assessment of public benefits.

A key issue will be the way the ACCC assesses mergers involving converging modes of content delivery. In clearing the proposed joint bid for interests in Ten Network Holdings Limited by Birke Pty Ltd and Illyria Nominees Television Pty Ltd in July 2017, the ACCC considered convergence between different modes of content delivery, but did not form a concluded view as to whether free to air TV, print newspapers and online news sites were in the same or different product markets. The converging nature of different modes of content delivery is an issue that the ACCC will continue to face in future mergers.

2. Impact of technological change

The media sector is inherently dynamic. The ACCC will assess media mergers in light of potential changes over the foreseeable future (typically one or two years). In doing so, the ACCC may consider the scope for technological convergence in that timeframe as well as market innovations that may facilitate competitive entry. However, the ACCC will require credible evidence that such changes will occur and gives little weight to mere speculation.

Similarly, the ACCC will consider the disruptive effects of new technologies. The ACCC may give disproportionate weight to new market entrants with low market shares if there is credible evidence that such firms

will quickly become vigorous and effective competitors. In doing so, the ACCC may look at international trends and examples.

While digital disruption has been viewed as a key driver of competition, the mere presence of digital competitors may not resolve all ACCC concerns. For example, the proposed merger between APN Outdoor and oOh!media was abandoned after the ACCC expressed concerns with competition in the out-of-home advertising market. The ACCC considered that online platforms were not a substitute for traditional billboards.

3. Access to key content

The ACCC has historically considered that insufficient access to premium or compelling content can be a barrier to entry. Such premium content can have a 'halo' effect and attract significant number of customers. Consequently, such content may be subject to exclusive supply arrangements that favour larger providers with deeper pockets at the expense of smaller market entrants.

In considering mergers, the ACCC will consider the extent to which the merger may foreclose third party competitors from acquiring access to key content, thereby reducing competition. This is not a new consideration for the ACCC. For example, Foxtel provided an undertaking to address ACCC concerns about access to exclusive content to proceed with its purchase of Austar in 2012.

The ACCC will also consider the way content holders may have countervailing power such that they may choose alternate platforms for their content.

4. Two-sided markets and network effects

A two-sided market is one in which a platform or intermediary brings together two distinct groups of users which interact with each other. Two-sided markets often arise in the context of services which generate revenue through advertising. Many Internet services involve two-sided platforms, often in the context of a free service. For example, Google provides a free 'search' function to consumers, but simultaneously sells advertisements for a profit to advertisers that can advertise to those consumers.

Network effects are present in a market if the value a user places on a product or service increases if there are more overall users of that product or service. For example, the benefit to an individual user from using a social networking site increases if all their friends also use that site. Network effects can raise the barriers to entry and expansion and impede effective competition from developing. In such cases, the 'winner takes all'.

By raising barriers to entry, network effects may be important in assessing the competitive effects of some media mergers. The level of such barriers to entry may depend on the context. Platform-to-platform competition, for example, can sometimes be viewed as competition *for* the market rather than *in* the market if the network effects are sufficiently transient.

5. Bundling and foreclosure

Bundling (or tying) refers to the practice of supplying or offering to supply complementary products as a package. The practice of bundling may be efficient, and the ACCC is only concerned where these strategies are likely to have the effect of substantially lessening competition. Cross-platform media mergers may provide the merged entity with the opportunity to bundle or tie the supply of products or services, for example content or advertising opportunities, across multiple platforms.

The ACCC will also closely examine any media merger that enables the merged entity to leverage its market power in one market to substantially lessen competition in another market. For example, a vertical merger between a content supplier that produces premium content and a free-to-air network may raise competition concerns if rival networks or competitors on other platforms need access to premium content to compete effectively.

Watch this space...

The reforms to the media cross-ownership rules are to be welcomed in a media sector that is undergoing profound change. The reforms create opportunities for further consolidation in the Australian media sector to enable traditional media companies to respond to competition from innovative new media.

The removal of two of the statutory restrictions means that the ACCC's role will become more visible than has historically been the case. The ACCC has responded by updating its Guidelines. The Guidelines are sensible, but illustrate some of the complexities that the ACCC will face when assessing dynamic markets that are subject to continued innovation and convergence. Watch this space...

CAMLA YOUNG LAWYERS

NETWORKING EVENT

WEDNESDAY 14th MARCH

The Communications and Media Law Association (CAMLA) Young Lawyers are holding a networking event for law students and young lawyers with an interest in the media and communications industries.

The panel will discuss their career paths, professional highlights & challenges and some tips on successful networking.

Jonathan Carter - Head of Legal, Corporate & Policy at APRA/AMCOS

Matthew Lewis - Barrister at 5 Wentworth Chambers

Kirsty McLeod - Senior Legal Counsel at TEN

Cate Nagy - Partner at King & Wood Mallesons

The finalists of the **CAMLA essay competition** will also be announced.

Where: **King & Wood Mallesons**
Dexus Place
Governor Macquarie Tower
Level 15, 1 Farrer Place, Sydney

When: **Wednesday 14th March**
6:00pm for a 6:30pm start
(followed by drinks and nibbles)

Tickets: **$25.00 (incl GST)**

Register: https://www.camla.org.au/seminars

Enquiries: camla@tpg.com.au **or (02) 4294 8059**

Rights Holders Rearmed with Preliminary Discovery Powers by Full Federal Court

Richard Hoad, Partner, and Sarah Martine, Lawyer, at Clayton Utz consider the recent Federal Court decision, which should ensure that the preliminary discovery process remains a real weapon in the armoury of rights holders who suspect that their rights are being infringed.

How can a party assess if litigation is worth the cost before launching it? Preliminary discovery is a mechanism by which a prospective applicant, which considers that it might have a legal claim against another party, can obtain relevant documents prior to the commencement of substantive proceedings, in order to assess the merits of its potential claim. But what must the applicant show?

The Full Federal Court decision of *Pfizer Ireland Pharmaceuticals v Samsung Bioepis AU Pty Ltd* [2017] FCAFC 193 makes it clear that a prospective applicant seeking an order for preliminary discovery only needs to have a reasonable belief that it **may** have the right to obtain relief from a prospective respondent.

Pfizer is concerned about potential patent infringement

The applicants (**Pfizer**) manufacture ENBREL, which is a biological medicine that is used in the treatment of autoimmune diseases such as rheumatoid arthritis, juvenile rheumatoid arthritis and psoriatic arthritis. The active ingredient in ENBREL is etanercept.

In July 2016, Samsung Bioepis AU Pty Ltd (**SBA**) obtained registration on the Australian Register of Therapeutic Goods of two pharmaceutical products containing etanercept as their active ingredient under the name BRENZYS. Pfizer was concerned that the manufacture of BRENZYS might infringe one or more of Pfizer's process patents. However, it did not have sufficient information to decide whether to commence patent infringement proceedings.

Faced with this dilemma, Pfizer utilised the Federal Court's preliminary discovery procedure. Pfizer sought preliminary discovery of certain documents that SBA lodged with the Therapeutic Goods Administration regarding the processes used to manufacture BRENZYS. Pfizer believed that these documents would enable it to decide whether or not to commence proceedings against SBA for patent infringement.

Preliminary discovery in the Federal Court

The relevant preliminary discovery procedure in the Federal Court is governed by Rule 7.23 of the Federal Court Rules 2011 (Cth), which allows a prospective applicant to apply to the Court for an order for discovery by a prospective respondent if the prospective applicant:

- has a reasonable belief that it has the right to obtain relief in the Court from a prospective respondent;
- after making reasonable inquiries, does not have sufficient information to decide whether to start proceedings to obtain such relief; and
- reasonably believes that the prospective respondent has, or is likely to have, in its control documents directly relevant to the right to obtain the relief, and that inspection of the documents would assist in making the decision.

How the Court assessed Pfizer's evidence to support its application for preliminary discovery

The key issue before the Federal Court was whether the expert evidence that Pfizer put forward in support of its application showed that Pfizer reasonably believed that SBA might be infringing its patents. Dr Ibarra (Pfizer's Director and Group Leader of Process Development, Manufacturing Science and Technology) provided expert evidence relating to the technical aspects of the patents and the process dependence of biological medicines.

At first instance, Justice Burley refused Pfizer's application. He was not satisfied that Pfizer had demonstrated that it had a reasonable belief, as opposed to a "mere suspicion", that it may have the right to obtain relief from SBA for patent infringement, saying that the mere fact that BRENZYS and ENBREL are biosimilar products does not mean that the manufacturing processes for the products are the same.

On appeal, the Full Court considered the proper approach to be taken in relation to preliminary discovery applications and, in particular, the "reasonable belief" requirement.

Three separate judgments were delivered, however there was broad agreement on the principles and Pfizer's appeal was unanimously upheld. The Full Court held that the evidence presented by Pfizer was sufficient to establish that it had a reasonable belief that it **may** have a right to obtain relief from SBA for patent infringement. As such, SBA was ordered to provide the discovery sought by Pfizer.

Requirements for preliminary discovery

Chief Justice Allsop observed that the language used in Rule 7.23 should be given its ordinary meaning and its wording used as the framework of analysis for deciding preliminary discovery applications. Any judicial guidance should not be elevated above this statutory formulation,

Bearing this in mind, Justice Perram provided the following useful guidance in relation to the requirements for seeking preliminary discovery:

- the prospective applicant must prove that it has a belief that it **may** (not **does**) have a right to relief;
- the prospective applicant must demonstrate that the belief is reasonable, either by reference to material known to the person holding the belief, or by other material subsequently placed before the Court;
- a person deposing to the belief need not give evidence of the belief a second time, to the extent that additional material is placed before the Court on the issue of the reasonableness of the belief;
- the question of whether the belief is reasonable requires asking whether a person apprised of all of the relevant material could reasonably believe that they **may** have a right to obtain relief;
- one may believe that a person may have a case on certain material without one's mind being in any way inclined to the notion that they do have such a case; and
- in practice, in order to defeat a claim for preliminary discovery, it will be necessary either to show that the subjectively held belief does not exist or, if it does, that there is no reasonable basis for thinking that there may be (not is) such a case.

Chief Justice Allsop noted, with apparent disapproval, that the application at first instance involved two days of hearings, and the application for leave and the appeal took a further two days. As the Chief Justice observed, the level of fact finding that took place was well beyond what was required by the language used in Rule 7.23.

Why this decision on preliminary discovery is good news for rights holders

The purpose of preliminary discovery is to enable a party to ascertain, in a reasonably efficient and cost-effective manner, whether the costs of substantive litigation are justified. As Chief Justice Allsop emphasised in this case, applications for preliminary discovery are summary in nature, and are not "mini-trials".

That purpose would be defeated if the process of applying for preliminary discovery was too burdensome or the hurdles were set too high – and, in particular, if the Court applied too rigorous a standard in the assessment of whether the applicant has a reasonable belief that it has the right to obtain relief. By definition, the prospective applicant has imperfect knowledge about the prospective respondent's conduct. The forming of the requisite belief will necessarily entail an element of speculation. The key question, as the Full Court recognises, is whether the belief which is formed is a reasonable one.

The Full Court's decision should ensure that the preliminary discovery process remains a real weapon in the armoury of rights holders who suspect that their rights are being infringed. It should also put a brake on the tendency for applications of this kind to become unnecessarily drawn out and costly.

Anti-money Laundering and Counter Terrorism Financing Requirements Extended to Cryptocurrency Exchanges

Nick Karagiannis, Partner, Luke Dale, Partner, and Daniel Kiley, Senior Associate, at HWL Ebsworth, consider new regulation of cryptocurrencies.

Money laundering is widely recognised as a key enabler for criminal activity, and the recent rise of pseudonymous cryptocurrencies has created new ways for this occur. Existing Australian laws in relation to money laundering were not fully equipped for these developments, but amendments have been passed by Parliament to address such matters.

These will commence shortly following a brief period of consultation. While the amendments place requirements on organisations running services to exchange traditional money for cryptocurrencies (or vice versa), and are designed to catch questionable activity, they will also potentially lessen the anonymity that everyday cryptocurrency users and investors would ordinarily expect.

The Australian Criminal Intelligence Commission (**ACIC**) recognises money laundering as one of the 'key enablers' for serious and organised crime in Australia. In its 2017 Organised Crime in Australia report, the ACIC stated that:

Money laundering remains a key risk to Australia and is the common element in almost all serious and organised crime. Money laundering enables criminals to hide and accumulate wealth, avoid prosecution, evade taxes, increase profits through re-investment, and fund further criminal activity. Money laundering activities also have the potential to undermine the stability of financial institutions and systems, discourage foreign investment and alter international capital flows.

The *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (**Act**) accordingly establishes a system of reporting obligations on financial institutions and other designated service providers, whereby certain transactions must be notified to the Australian Transaction Reports and Analysis Centre (**AUSTRAC**). Relevant institutions are also required to verify a customer's identity before providing certain services to customers.

While the Act already has mechanisms in place to address large movements of money via traditional banking systems, it was underequipped to deal with issues that arise with respect to cryptocurrencies. This is of particular concern given that the ACIC has also reported that:

The two key enabling technologies currently used to facilitate serious and organised crime are virtual currencies and encryption. Virtual currencies, such as bitcoin, are increasingly being used by serious and organised crime groups as they are a form of currency that can be sold anonymously online, without reliance on a central bank or financial institution to facilitate transactions.

As such, on 7 December 2017 Commonwealth Parliament passed the *Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2017* (Cth) to bring digital currency exchanges (where traditional money can be exchanged for cryptocurrencies) within the scope of the Act, along with a number of other amendments.

Under the Act prior to these amendments, there was a concept of an *e-currency,* being a digital currency backed directly or indirectly by a precious metal or bullion. Plainly, this did not apply to the majority of the cryptocurrencies that are becoming increasingly popular, which generally are not backed by physical items in this way. Accordingly, a new and much broader defined term, *digital currency,* has been inserted.

As part of the changes to the Act, digital currency exchanges operated in Australia or by an Australian person or entity will be required to:

- register with AUSTRAC;
- adopt and maintain an Anti-Money Laundering/Counter-Terrorism Financing program to identify, mitigate and manage associated risks;
- identify and verify the identities of their customers;
- report all transactions with a value exceeding $10,000 or more, along with any other suspicious activities, to AUSTRAC; and

- keep certain records of transactions, identities and Anti-Money Laundering/Counter-Terrorism Financing programs for at least seven years.

The precise matters to be reported to AUSTRAC are still to be finalised, as they are specified in a set of Rules made under the Act. AUSTRAC released a draft set of these Rules for public consultation on 16 January 2018, and submissions closed on 13 February 2018.

Under the Rules as currently proposed, reports to AUSTRAC on digital currency matters would include a range of standard details about the identity of the individual involved and the money sent or received, but also, uniquely to digital currency transactions, include:

- Internet Protocol (**IP**) addresses;
- email addresses and phone numbers;
- social media usernames;
- unique identifiers relating to the digital currency wallets (such as the public address of a wallet); and
- unique identifiers of devices involved, including Media Access Control (**MAC**) addresses, International Mobile Equipment Identity (**IMEI**), International Mobile Subscriber Identity (**IMSI**) numbers, and secure element ID (**SEID**) numbers.

The amendments to the Act only operate at the fringes of cryptocurrency networks, by capturing transactions that see traditional currency exchanged for virtual currencies and vice versa. However the pseudonymous public ledgers that form part of most cryptocurrencies (including Bitcoin, for example), allow anyone to observe the movement of funds between public wallet addresses. As wallet addresses are to be provided to AUSTRAC under the draft Rules, this should theoretically allow it some visibility over the movement of funds after they take digital form.

While many like to think of cryptocurrencies as anonymous, this is typically not the case, with the wallet addresses associated with each user serving to pseudonymously identify them. With the reporting of wallet addresses to AUSTRAC, it should, over time, be able to amass a database of the real identities associated with otherwise pseudonymous wallet addresses. This may assist in discouraging the use of cryptocurrencies for black market transactions. However, many enthusiasts are likely to see it as going against the liberal ideals on which many cryptocurrencies were founded.

Newer cryptocurrencies have launched with different technologies that promise greater anonymity, which may become more appealing to users as government oversight increases through measures such as these changes to the Act.

The amendments to the Act, and associated new Rules, are expected to commence on 1 April 2018.

This article was written by **Nick Karagiannis,** Partner, **Luke Dale,** Partner, and **Daniel Kiley,** Senior Associate at HWL Ebsworth.

About CAMLA

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

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

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

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

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

Disclaimer

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

For further information:

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

To: The Secretary, camla@tpg.com.au or CAMLA, PO Box 345, HELENSBURGH NSW 2508

Phone: 02 42 948 059

Name:

Address:

Telephone: Fax:

Email:

Principal areas of interest:

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

☐ Ordinary membership $130.00 (includes GST)

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

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

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