CAMLA COMMUNICATIONS LAW
BULLETIN
Communications & Media Law Association Incorporated
Volume 37, No 2. May 2018

Interview with Geoffrey Robertson QC

It is difficult to introduce a person who requires no introduction. It compounds my difficulty to do so while, in that most lawyerly fashion, avoiding any use of superlatives. So permit me please this "one" editorial indulgence. Give or take Doc Evatt, as one doesn't, Geoffrey Robertson QC may well have achieved more for the causes of human rights and free speech globally than any Australian lawyer to date. Geoffrey is one of the primary authors of Media Law – and I'm not just referring to his textbook of that name.

His resume reads as but a succulent synopsis to his brilliant memoirs, released in February this year, *Rather His Own Man*, which are truly required reading.

After completing his law degree at Sydney University, Geoffrey followed a Rhodes Scholarship to Oxford, and was called to the UK bar shortly after. He would go on to found, and continues to head, Doughty Street Chambers, chambers, which are now second best known for their ground-breaking human rights work. He has appeared as leading counsel in over 200 reported cases, many in the European Court of Human Rights, the House of Lords, the UK Court of Appeal, the UK High Court and the Privy Council, as well as in appellate courts in Singapore, Trinidad, Malawi, Mauritius, New Zealand, Fiji, Malaysia and the Eastern Caribbean – and here in Australia (more about that below). Throughout his illustrious career, Geoffrey has consistently been involved in some of the most high-profile media law cases internationally. He has acted for CBS, Dow Jones, The Sunday Telegraph, Forbes Magazine, the New York Times, Time Magazine and Fortune Magazine. He was also called to defend Salman Rushdie in blasphemy proceedings, and Julian Assange in extradition proceedings in the UK. And yet, we are barely scratching the surface.

FISHER: Geoffrey, thank you so much for taking the time to sit down and discuss all things media law with me. On behalf of our readers, I'm grateful for your insights!

ROBERTSON: Well, thank you for that overkind introduction. I'm just a jobbing barrister, really. But I do go back a long way – when I wrote the first edition of 'Media Law,' over 30 years ago, it is amazing to think that the title had never been used before. There was defamation and contempt, and obscenity and copyright, and so on, but they were entirely different legal subjects ununified by principles like freedom of expression and open justice.

FISHER: You write in *Rather His Own Man* that you have always been a journalist manqué. I suspect that tossing up between a life in the media and one in media law is not an uncommon dilemma for media lawyers. Can you tell us more about what drove you to media law?

Continued on page 3 >

Contents

CAMLA

Editors
Victoria Wark & Eli Fisher

Editorial Assistant
Imogen Yates

Printing & Distribution
BEE Printmail

Editors' Note

Well, first, may we wish you all a merry Privacy Awareness Week and a happy World Intellectual Property Day!

In early March of this year, we published the previous edition - the first of 2018. And, what a few months it has been since!

The EU's game-changing privacy law, the **GDPR**, is coming into effect on 25 May 2018, and it affects Australian businesses. More about that inside. The Government responded to the **Productivity Commission**'s report on data availability and use. The OAIC released its report on **Data Analytics and the APPs**, and its first quarterly report on the mandatory notifiable data breach scheme, finding that in about two months, 63 data breaches had been notified, as compared to 114 on a voluntary basis for the whole 16-17 financial year. Almost a quarter of notifications came from the **health service providers** industry. More about that inside.

Information came to light about the way **Cambridge Analytica** was processing information collected from **Facebook**, which caused a bit of stir. Users moved to publicly #DeleteFacebook in a protest. Class action suits were commenced. Mark Zuckerberg was summoned to testify before Congress. Regulators around the world are investigating. Here, the Privacy Commissioner opened an investigation on 5 April 2018, and the Australian Competition and Consumer Commission is shifting the focus of its digital platforms inquiry to privacy protection and the fairness of Facebook's terms and conditions. Facebook shares plummeted in the week and a half after the revelations, proving once and for all how costly it is to not comply with privacy law. Then, a couple of months later, they went back up to what they were previously - proving that there either is or isn't a moral to this story. More about Facebook inside.

On the topic of the **ACCC inquiry into digital platforms**, submissions have been published. There were 57 in total, including contributions from most major Australian media organisations, industry bodies, unions and advertisers. In a 144-page submission, **News Corp** submitted that a number of digital platforms possess substantial market power and are engaging in anti-competitive practices that prevent publishers from competing on the merits. The **MEAA** estimated that since 2011, a quarter of all journalists in Australia have been made redundant. **Foxtel** complained of "unauthorised hosting and distribution of copyright material by digital platforms, material that is created and paid for by the platforms' competitors", and gave examples of Fox Sports content available on YouTube.

In the Government's **competitive neutrality inquiry**, the expansion of the ABC's online news service, ABC iView, SBS On Demand and other services, is being examined in light of complaints from Foxtel, News Corp and Fairfax about taxpayer-funded media crowding them out.

Dodo, **iPrimus** and **Commander** have undertaken to offer remedies to customers who couldn't receive the internet speeds they bought because their **NBN** connection was incapable of delivering it. The **ACCC** has separately commenced proceedings against **Telstra**, alleging that false or misleading representations were made to consumers in relation to its third-party billing service known as Premium Direct Billing. It appears the parties have agreed to consent orders, which involve Telstra paying pecuniary penalties totalling $10 million.

On the defamation front, the jury in **Sophie Mirabella**'s claim against the **Benalla Ensign** held that an article that she pushed **Cathy McGowan** was defamatory. **Geoffrey Rush** succeeded in preventing **Nationwide News** joining the **Sydney Theatre Company** as a co-defendant in the proceedings, although the Court did not rule out Nationwide News seeking to pursue the Sydney Theatre Company for contribution by way of separate proceedings. And **Stormy Daniels** is suing **Donald Trump**.

In this edition, we have a chat with **Geoffrey Robertson QC** about free speech, censorship and defamation. **Demetrios Christou** and **Eva Lu** from Thomson Geer discuss the Cambridge Analytica story. **Peter Leonard** from Data Synergies gives us the second part of his thoughts on the new data breach law, this time taking us through data breach laws around the world. Over at Allens **Valeska Bloch** sets out some of the issues to arise out of the mandatory data breach notification scheme, and **Gavin Smith**, **Jessica Selby** and **Claudia Hall** discuss the implications of the Federal Government's response to the Productivity Commission's report on data availability and use. **Michael Boland** interviews Seven's commercial director, **Bruce McWilliam**. We have two pieces from our friends at MinterEllison, the first by **Veronica Scott** and **Ashleigh Fehrenbach** on the GDPR, and the second piece about the cabinet papers scandal from **Katherine Giles**. Two of our essay competition's finalists are published: **Penelope Bristow** on the challenges of defamation law in a social media environment, and **Claudia Carr** on Net Neutrality in Australia.

Victoria and Eli

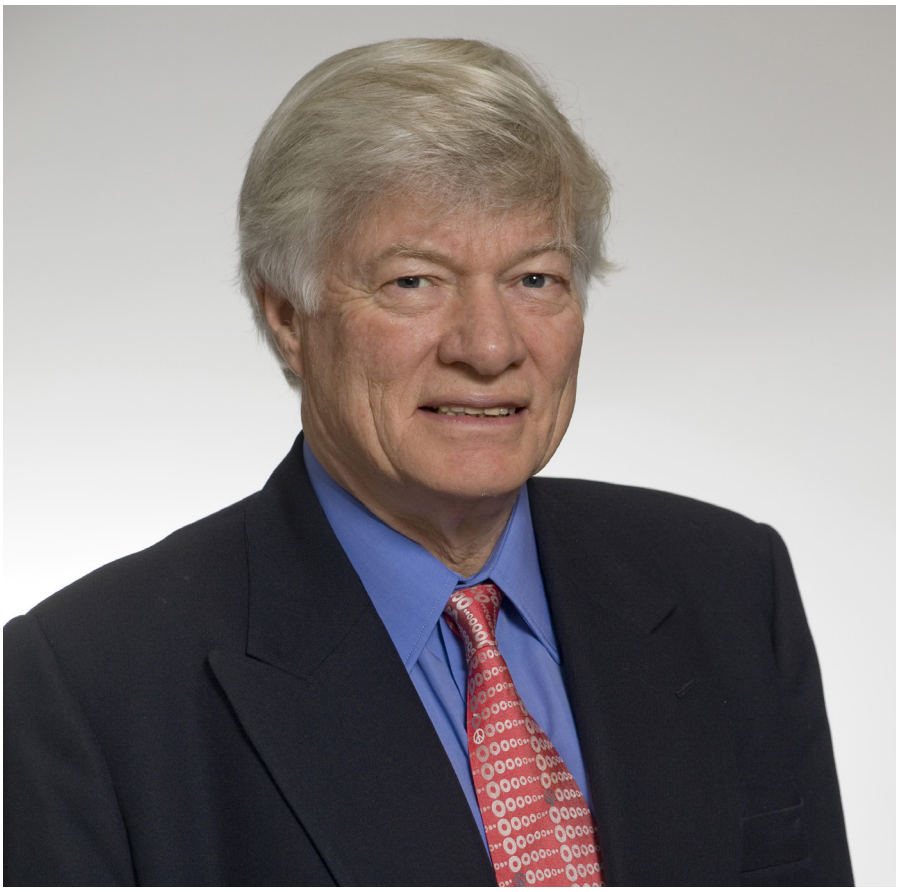
ROBERTSON: I was always – from my teenage years – fighting against censorship, and at the same time I was interested in journalism. I wrote for 'The New Statesman' and 'The Guardian' whilst studying for bar exams. I guess I was interested in exploring the similarities between these apparently disparate subjects – obscenity, defamation, contempt and so on. I began with obscenity – the OZ case – and then moved on to contempt and libel, always trying to argue, sometimes to create, public interest defences. My most important client was the Wall Street Journal – 'The American Lawyer' called me 'Dow Jones man about the Commonwealth' – and they were very principled about fighting for free speech, even in Singapore where it was impossible to win against Lee Kuan Yew.

FISHER: Was your passion for human rights born from your work in defence of free speech and a free press, or was it simply a separate devotion for you?

ROBERTSON: I don't think you can separate freedom of expression from other human rights. I started doing death penalty cases at the same time, and some of my most important appellate victories have concerned due process. They are all, in a way, about life, liberty and the pursuit of happiness.

FISHER: You talk of your "pommified" accent in your book. But you have always proudly considered yourself Australian as well, especially during the Ashes (current tumults in Australian cricket notwithstanding). What impact did your upbringing in Australia have on your life in law, practising predominantly in the UK?

ROBERTSON: That's a good question, and I am not sure of the answer, other than that my American clients - journalists and editors – found it strangely reassuring that despite my accent and my English QC-ship, I was really Australian. English barristers tend to come across as upper-class, snobbish and stiff-shirt, traits Americans do not associate with Australians.



FISHER: The title of your memoirs "Rather His Own Man" derives from a comment, intended but not quite received as derogatory, which a Permanent Secretary made to a Minister who was intending to propose your appointment to an important European judicial position. In other words, you could not be trusted always to do what the government might want. Later in your book, you liken one of your clients Julian Assange – another Australian – to "that swagman in 'Waltzing Matilda', determined not to be taken alive, even if it means living in a converted toilet in the Ecuadorian embassy. Is there, in your experience, something inherently Australian about nonconformism?

ROBERTSON: Australians like to think so, but when I grew up there we seemed to be the most conformist country of all. It's really a myth, like thinking we are an egalitarian country because we ride in the front seat of taxis. It's a delusion really.

FISHER: You consulted to the Australian Government on defamation law reform in 1984, and have been involved in defamation work in Australia throughout your career, starting out sitting behind the likes of Tony Larkins and Clive Evatt as an articled clerk, and arguing for Dow Jones in the High Court, in the case brought by Joe Gutnick in 2003. There are some lingering irritants about Australian defamation law for you though. In particular, there is no public interest defence in defamation. Based on your experience, why is such a defence so important and how should it work?

ROBERTSON: I think Australian law really lags here, in this respect. The High Court did a great thing by drawing 'democratic implications' out of the constitution, permitting free speech in 'political matters,' but we need free speech in other areas, especially about business. Countries like Britain and New Zealand and Canada have public interest defences based on freedom of expression clauses in their Bill of Rights – we have no such equivalent. But I think the other systemic problem in Anglo-Australian libel law is the burden of proof being placed on the media defendant. In every other

branch of civil law those who bring the claim have to prove it. That is why US courts will not enforce Australian libel judgements, thanks to a case – *Bachchan v India Abroad* – in which I gave expert evidence and the judge said that forcing the defendant to prove truth, fair comment, etc. was 'antipathetic to the first amendment.' We will never get defamation law right in this country until the burden of proof is placed on the plaintiff.

FISHER: Another source of frustration for you is the relative lack of protection for a journalist's sources. What experiences have you had in other jurisdictions that reinforce how important such protections can be?

ROBERTSON: Well, I argued *Goodwin v UK*, the most important case on the subject, in which the European Court of Human Rights accepted that there would be a lot less news of public interest if journalists could not protect their sources. The rule applies now in 47 European countries, but not in Australia – another aspect in which media law in Australia is defective.

FISHER: Coming back to *Gutnick v Dow Jones,* a decade and a half down the track, and with the internet considerably more developed and better understood, was it the right decision?

ROBERTSON: No, and it's been politely 'distinguished' by courts in other countries. The judges on the High Court at the time could not distinguish between a newspaper and the internet, and I failed to enlighten them.

FISHER: You were involved in the *Spycatcher* case, with another talented Australian media lawyer. Can you tell us the story there, and what that has taught you about attempts by the state to censor works of art and literature?

ROBERTSON: I gave Malcom Turnbull the case, which was the making of him and so I guess I am responsible for his rise and rise. But you know why I gave him the case? Because all the other so called 'media lawyers' we tried, in Melbourne and Sydney, were utterly hopeless. They were ignorant of the free speech principles, and they said we had no chance in Australia. I hope they are better now, 30 years on. The 'Spycatcher' effect now stands for the proposition that censorship is counter-productive: it just sells more books.

FISHER: Part of the curse of a legal trailblazer is having to make arguments without being able to rely on precedent. In fact, you have been criticised by some courts for bringing what they consider to be airy-fairy arguments about free speech without reliance on precedent or statute. How do you advise clients about the merits of an untested argument, and how do you personally deal with the stress of making it?

ROBERTSON: It's less of a problem nowadays because most counties in which I appear have Bills of Rights or constitutional guarantees of free speech, and even in Australia we are party to UN treaties and can cite judgments from the UN Human Rights Commission and so on. Some judges remain absurdly insular, like the fellow I struck in Victoria in the *Gutnick* case, but most are receptive and prepared to consider ways that other courts in other countries have approached the same problem.

FISHER: You were inspired to be a barrister by the *Trial of Lady Chatterley.* An aversion to censorship, especially of works of a sexual nature, has driven you to defend the freedoms of artists and authors throughout your career, which included you writing your text on the matter, *Obscenity.* Your protest against censorship famously caused the Canadian authorities some embarrassment, if memory serves me. Why is censorship such a concern for you – and where should the line be drawn?

ROBERTSON: Censorship issues have changed. When I started, the battle was against the wowsers, the puritans in power around the world, whose decisions might be challenged by a jury verdict. We won freedom for good literature and then for bad or amateur literature, but now with Snowden and Assange the battle is over information. There are still too many areas covered up by Freedom of Information exemptions.

FISHER: Why was *Jameel* so important for you, and what do you hope develops in its wake?

ROBERTSON: There are two *Jameel* cases. One – which has caught on – is that disproportionate claims should be stayed, or struck out. The other, more important, is that a public interest privilege defence should apply to incidental defamation – i.e. when the story itself has public interest and the defamatory statement is reported not because the imputation is true but because the statement was made and was newsworthy. In the UK, *Jameel* has led to useful changes in the law – a new defamation act which excludes inconsequential libels and a reasonably strong public interest defence. It was a case we lost at Trial and in the Court of Appeal – thank goodness we had clients like the Wall Street Journal prepared to hazard millions on a win in the House of Lords! Free speech can be expensive speech.

FISHER: What challenges lie ahead for free speech? What work will media lawyers be consumed by in the coming years?

ROBERTSON: The problem now in Europe and the US is privacy, and the role of journalism as propaganda, and the ability of propagandists to sway democratic choice – see the Cambridge Analytica scandal. There will be plenty for media lawyers to do in the future!

FISHER: Geoffrey, thank you so much for your time. We are grateful for the work you do, and for your spending the time to tell us about it.

ROBERTSON: My pleasure.

How Will Consumers Value the Data They Provide After the Cambridge Analytica Revelations?

Demetrios Christou (Partner) and Eva Lu (Lawyer) at Thomson Geer consider the recent developments from the Facebook and Cambridge Analytica revelations.

What started as a simple personality quiz has resulted in Facebook being investigated by regulators around the world, including our own, and has landed Mark Zuckerberg, its CEO, in front of the US Congress to face questions on Facebook's data privacy practices.

So what happened, what was the fallout, what do our privacy laws say and at the end of the day, why should we care?

What happened?

The details about what happened first came to light in March when reporters from The Observer[1] published a story following a year-long investigation into Cambridge Analytica's involvement in the US elections.[2] Keep in mind that the details about what happened are still evolving and a lot about what we know comes from the conflicting accounts of the parties involved.

While this story begins with a simple personality quiz, the details surrounding the revelations are far more complex.

In 2014, Cambridge University researcher Aleksandr Kogan, through his company Global Science Research (**GSR**) developed a Facebook app called "thisisyourdigitallife". The app was downloaded by around 270,000 users and each user was paid $1 - $2 to take the app's personality test.

GSR used the app to collect personal information about those users purportedly for "academic purposes". As well as collecting information on each user, GSR also collected information about each user's Facebook friends, leading to the accumulation of a data pool, which according to Facebook, affected up to 87 million people.[3] While users of the app will likely have given consent to the collection and use of their personal information, the friends of those users would not have had the opportunity to consent to their personal information being collected or shared in this way.

The app collected the data through Facebook's first iteration of its Graph API. This is essentially a Facebook tool that was made available to third party app developers giving them access to a vast amount of data about Facebook users and their friends. The first version of the tool was made available to developers in 2010. Facebook started to phase it out in April 2014 until it was completely closed in 2015 after Facebook saw problems with the amount of data available through the tool.[4] A second iteration was implemented which was more restrictive in the data it made available.

GSR reportedly supplied the data from the app to Cambridge Analytica and SCL Elections (**SCL**), the parent company of Cambridge Analytica at the time.[5] Facebook's policy at the relevant times only allowed the collection of a user's friends' personal information through the Graph API to improve user experience on the platform. It did not allow it to be used or shared for advertising purposes.[6]

In 2015, after discovering the enormous amount of data that had been collected using the "thisisyourdigitallife" app, Facebook removed the app from its platform and demanded certification from GSR, and all parties that GSR had given the data to, that the data had been destroyed. In response Cambridge Analytica certified that it had destroyed the data in question. Apparently Facebook did not pursue the issue any further at that stage.[7]

On 16 March 2018 Facebook announced that it was suspending Cambridge Analytica and the SCL Group from its platform for failing to delete all the data it had received in 2015 from GSR as it had certified.[8] This action was

1 The Observer is a sister publication to The Guardian newspaper published on Sundays, both of which are published online through www.theguardian.com.

2 Carole Cadwalladr and Emma Graham-Harrison, 'Revealed: 50 million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach', *The Guardian* (online), 18 March 2018 <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>.

3 Mike Schroepfer, 'An Update on Our Plans to Restrict Data Access on Facebook' on *Facebook Newsroom* (4 April 2018) <https://newsroom.fb.com/news/2018/04/restricting-data-access/>.

4 Josh Constine, 'Facebook is Shutting Down its API for Giving Your Friends' Data to Apps', *TechCrunch* (online), 29 April 2015 <https://techcrunch.com/2015/04/28/facebook-api-shut-down/>.

5 Carole Cadwalladr and Emma Graham-Harrison, above n 2.

6 Ibid.

7 Ibid.

8 Paul Grewal, 'Suspending Cambridge Analytica and SCL Group from Facebook' on *Facebook Newsroom* (16 March 2018) <https://newsroom.fb.com/news/2018/03/suspending-cambridge-analytica/>.

purportedly taken after Facebook became aware of upcoming news stories from The New York Times[9] and The Observer.[10] On 21 March 2018, CEO Mark Zuckerberg released a public statement on his Facebook page laying out the timeline of events leading up to the revelations.[11]

Cambridge Analytica has strongly denied all allegations and agreed to a forensic audit by an independent third party. Cambridge Analytica in its 9 April 2018 press release[12] states that GSR "licensed the data to us, which they legally obtained via a tool provided by Facebook." In the same press release, Cambridge Analytica claimed that the data of only 30 million people was licensed from GSR. It noted that although it was involved in the Trump campaign, it did not use any of the data obtained from GSR. It also claimed that all data, including derivatives, was deleted when requested by Facebook.

What was the fallout?

Irrespective of what actually happened, the fallout was immediate. Facebook's shares fell within days of its announcement, wiping a total of $100 billion from its market value.[13]

The hashtag #DeleteFacebook appeared more than 10,000 times on Twitter within a two-hour period on the following Wednesday.[14] Facebook is now facing investigations from regulators around the world.[15] Lawsuits have been filed against Facebook and Cambridge Analytica by investors and individual users.[16] Both Cambridge Analytica and SCL have since announced that they will be closing down.[17]

In response to the reporting on the revelations, Zuckerberg took out full page ads in newspapers in the UK and US apologising for Facebook's role[18] and testified before a two-day US Congress inquiry. For Facebook, the backlash has been focused on its failure to police activities on its own platform and its lack of responsibility over the use of its user data. Facebook has since announced sweeping changes to many of its APIs.[19] It has disabled a form of advertising targeting called Partner Categories.[20] It has also undertaken significant overhauls of its privacy and security measures, including by making efforts to give users more control over those features and provide users with a tool to find, download and delete their Facebook data.[21]

What do our privacy laws say?

The acting Privacy Commissioner announced that it has opened a formal investigation into Facebook, following confirmation from Facebook that the information of over 300,000 Australian users may have been acquired and used without authorisation.[22] The investigation will consider whether Facebook has breached the *Privacy Act 1988* (Cth) (**Privacy Act**), which regulates the way organisations collect, use, handle and disclose personal information.

Under the Privacy Act, an organisation must collect personal information only by lawful and fair means[23] and only from the individual unless it is unreasonable or impracticable to do so.[24] The organisation also has an obligation to notify individuals that it has collected personal information about an individual.[25] There is little doubt that the personal information of friends of the users that downloaded the "thisisyourdigitallife" app was collected by GSR without any direct consent by the friends of those users.

When it comes to use or disclosure, if an organisation holds personal information about an individual

9 Matthew Rosenberg, Nicholas Confessore and Carole Cadwalladr, 'How Trump Consultants Exploited the Facebook Data of Millions', *The New York Times* (online), 17 March 2018 <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html>.

10 Carole Cadwalladr and Emma Graham-Harrison, above n 2.

11 Mark Zuckerberg, 'I Want to Share an Update on the Cambridge Analytica Situation [...]', Facebook Post, 21 March 2018 <https://www.facebook.com/zuck/posts/10104712037900071>.

12 Cambridge Analytica, '"Time for Facts not Conjecture" says Cambridge Analytica Chief' (Press Release, 9 April 2018) <https://ca-commercial.com/news/time-facts-not-conjecture-says-cambridge-analytica-chief>.

13 Lucinda Shen, 'Facebook Stock is in the Red for the Year After the FTC Confirms Investigation', *Fortune* (online), 26 March 2018 <http://fortune.com/2018/03/26/facebook-stock-ftc-investigation-cambridge-analytica/>.

14 Tiffany Hsu, 'For Many Facebook Users, a 'Last Straw' That Led Them to Quit', *New York Times* (online), 21 March 2018 <https://www.nytimes.com/2018/03/21/technology/users-abandon-facebook.html>.

15 Elton Gomes, 'Cambridge Analytica Scandal: Facebook Facing Investigations in Several Countries', *Qrius* (online), 7 April 2018 <https://qrius.com/cambridge-analytica-scandal-facebook-facing-investigations-from-several-countries/>.

16 Jonathan Stempel, 'Facebook, Cambridge Analytica Sued in U.S. by Users over Data Harvesting', *Reuters* (online), 22 March 2018 <https://www.reuters.com/article/us-facebook-cambridge-analytica-lawsuits/facebook-cambridge-analytica-sued-in-u-s-by-users-over-data-harvesting-idUSKBN1GX1XK>.

17 Olivia Solon and Oliver Laughland, 'Cambridge Analytica closing after Facebook data harvesting scandal', *The Guardian* (online), 2 May 2018 <https://www.theguardian.com/uk-news/2018/may/02/cambridge-analytica-closing-down-after-facebook-row-reports-say>.

18 Nick Statt, 'Mark Zuckerberg Apologises for Facebook's Data Privacy Scandal in Full-Page Newspaper Ads', *The Verge* (online), 25 March 2018 <https://www.theverge.com/2018/3/25/17161398/facebook-mark-zuckerberg-apology-cambridge-analytica-full-page-newspapers-ads>.

19 Kurt Wagner, 'Facebook will Stop Sharing as much of Your Personal Data with People Outside of Facebook', *Recode* (online), 4 April 2018 <https://www.recode.net/2018/4/4/17199354/facebook-stop-sharing-data-outside-app>.

20 Nick Statt, 'Facebook will no longer allow Third-Party Data for Targeting Ads', *The Verge* (online), 18 March 2018 <https://www.theverge.com/2018/3/28/17174854/facebook-shutting-down-partner-categories-ad-targeting-cambridge-analytica>.

21 Aric Jenkins, 'Facebook Just Revealed 3 Major Changes to its Privacy Settings', *TIME* (online), 28 March 2018 <http://time.com/5218395/facebook-privacy-settings-changes-cambridge-analytica/>.

22 Office of the Australian Information Commissioner, 'Investigation into Facebook Opened' (Statement, 5 April 2018) <https://www.oaic.gov.au/media-and-speeches/statements/facebook-and-cambridge-analytica>.

23 *Privacy Act 1988* (Cth), sch 1 APP 3.5 ('*Privacy Act*').

24 Ibid sch 1 APP 3.6.

25 Ibid sch 1 APP 5.1.

that was collected for a particular purpose, then the organisation must not use or disclose the information for another purpose unless the individual consents, or if an exception applies, such as if the individual would reasonably expect the use or disclose for another purpose and that purpose related to the original purpose.[26]

Cambridge Analytica has laid the blame on GSR from whom it licensed the data. It claims its contract with GSR stipulated that GSR should seek informed consents from those users for use of the data.[27] Cambridge Analytica also denies the data was ever used for advertising or political purposes during the Trump campaign. It is difficult to know how the data of these 87 million users was used, however, this may become clearer if Cambridge Analytica complies with an enforcement notice served on it by the UK Information Commissioner's Office (**ICO**).[28] The ICO's notice requested information about where it received data and how it used data about a US voter in a test case that may see more US citizens seek access to the data Cambridge Analytica holds about them.

However it was Facebook, through its Graph API, that disclosed the personal information of those users that downloaded the app and the personal information of their friends. The Privacy Commissioner's investigations will no doubt look into whether Facebook took appropriate measures to notify or procure informed consent from individuals about how their personal information could be disclosed to and used by those third parties through these tools.

Under the Privacy Act if an organisation holds personal information, the organisation must take such steps as are reasonable in the circumstances to protect the information from misuse, interference and loss, and from unauthorised access, modification or disclosure.[29] These obligations are central to the allegations that Facebook has breached our privacy laws. Irrespective of what GSR or Cambridge Analytica did with the information, Facebook had a clear obligation to protect the information of its users and subsequently to alert its users and recover the information once it discovered the breach. While Facebook took steps in 2015 to limit the data available through its Graph API, it will be interesting to see the results of the Privacy Commissioner's investigations in this regard.

Why should we care?

Does it matter whether or not Cambridge Analytica has deleted all the data? There are arguments that the data GSR collected can never really be deleted when the models built from the data seem to still be circulating and are being developed further.[30] However, this is irrelevant when considering whether there were breaches at the time of the collection, use or disclosure.

Is it possible that the micro-targeting techniques deployed using the GSR data significantly helped Trump win the election in 2016? Cambridge Analytica has denied that it used the data during the Trump campaign. That aside, there is limited evidence that proves micro-targeting actually works and its effectiveness has been questioned by marketers and advertisers.[31]

Even so, political profiling is nothing new. Researchers and academics have surveyed and profiled voters for decades.[32] However, this time the data was purportedly taken without consent and the vast amounts of data means GSR could create psychographic profiles of millions of users, which were much more detailed than the demographic profiles which have previously been used in voter profiling. Although whether this is true or not is not 100% clear either.[33]

Finally, is it that surprising that Facebook has allowed third parties to access and continues to allow them to access the personal information of its users? After all, this is fundamentally Facebook's business model and Facebook has been selling user data to advertisers for years. Recent pieces on "I downloaded all the data Facebook has on me" provides some eye opening insights into just how much data is able to be collected through the use of platforms like Facebook.[34]

But these are not likely to be the biggest concerns that consumers will have about Facebook, GSR or Cambridge Analytica. This is not a question about micro-targeting and how micro-targeting can manipulate elections to undermine the democratic process. This is not a question of how much personal information is out there or who is using it and how.

26 Ibid sch 1 APP 6.1 and APP 6.2.

27 Carole Cadwalladr and Emma Graham-Harrison, above n 2.

28 Carole Cadwalladr, 'UK regulator orders Cambridge Analytica to release data on US voter', *The Guardian* (online), 5 May 2018 < https://www.theguardian.com/uk-news/2018/may/05/cambridge-analytica-uk-regulator-release-data-us-voter-david-carroll>.

29 *Privacy Act* sch 1 APP 11.1.

30 Dell Cameron, 'AggregateIQ Created Cambridge Analytica's Election Software, and Here's the Proof', *Gizmodo* (online), 28 March 2018 <https://www.gizmodo.com.au/2018/03/aggregateiq-created-cambridge-analyticas-election-software-and-heres-the-proof/>.

31 Brian Resnick, 'Cambridge Analytica's "Psychographic Microtargeting": What's Bullshit and What's Legit', *Vox* (online), 26 March 2018 <https://www.vox.com/science-and-health/2018/3/23/17152564/cambridge-analytica-psychographic-microtargeting-what>.

32 Poppy Noor, 'There are Plenty more like Cambridge Analytica. I Know – I've Used the Data', *The Guardian* (online), 24 March 2018 <https://www.theguardian.com/commentisfree/2018/mar/23/plenty-more-like-cambridge-analytica-data-facebook>.

33 Matthew Hindman, 'How Cambridge Analytica's Facebook Targeting Model Really Worked – According to the Person who Built it', *The Conversation* (online), 30 March 2018 <https://theconversation.com/how-cambridge-analyticas-facebook-targeting-model-really-worked-according-to-the-person-who-built-it-94078>.

34 Ariel Bogle, 'I Asked Everyone from Facebook to Data Brokers to Stan for my Information. It got Messy', *ABC News* (online), 28 April 2018 <http://www.abc.net.au/news/science/2018-04-28/i-asked-everyone-for-data-from-facebook-to-data-brokers-to-stan/9676700>.

Instead the biggest concern that consumers are now likely to have in light of these revelations is how much control has been relinquished over how their personal information is used and disclosed.

The Facebook Graph API was a revolution at the time in large-scale data collection because it allowed user data to be made much more economically available to third parties. It literally converted users and their likes, shares, connections, locations, updates and extended social networks into "objects" that app developers could request and take out of Facebook.[35] It is not difficult to regard users' data as a "product" when the Facebook Graph API refers to those data points as being "objects" when it makes those data points available for use by app developers.

One of the most revealing moments from the US Congressional hearings was Mark Zuckerberg's response to Senator Hatch's question of "... how do you sustain a business model in which users don't pay for your service?" - "Senator, we run ads." While targeting advertising is the direct source of Facebook's income, attributing to 98% of its revenue,[36] the targeted advertising purchased by advertisers is only effective because of the data that consumers freely share with Facebook.

In light of this, if consumers consider themselves from the perspective of a supplier of a product (i.e. their data) and not a consumer of a 'free' service, then they might begin to consider what sort of returns and protections they should demand for the products they supply and consider the possibility of taking that product away if their demands are not met. Perhaps one of those demands could be more control over their personal information.

Facebook's recent privacy setting changes appear to provide further protections, but the devil is in the detail. Facebook gives users control over what they actively choose to post or share, but users have no control over what is passively shared about them, or the information third parties can query and extract through various Facebook tools. Facebook continues to retain all control over the design and operation of their APIs. Facebook also appears to be making plans to change its terms of service in May so that 1.5 billion of its members, including those in Australia, will not fall under Europe's new General Data Protection Regulation.[37]

Whether all this results in a reduction in the use of platforms like Facebook is unlikely, but as we have seen following the reporting on the revelations, the loss of the public's trust in an organisation can have far reaching consequences beyond the direct legal implications.

Conclusion

The Facebook and Cambridge Analytica revelations have highlighted the extent to which the personal information of individuals can be used and the true price that consumers pay for the use of 'free' services. It will be interesting to see what findings come out of the acting Privacy Commissioner's investigation into Facebook, Cambridge Analytica's response to the ICO's enforcement notice and whether the revelations will have any impact on the current Australian Competition and Consumer Commission inquiry into digital platforms. But more importantly, what steps, if any, Facebook and other data gathering platforms will take to improve their information handling practices in light of the longer term public response to such findings.

35 Jonathan Albright, 'The Graph API: Key Points in the Facebook and Cambridge Analytica Debacle', *Medium* (online), 21 March 2018 <https://medium.com/tow-center/the-graph-api-key-points-in-the-facebook-and-cambridge-analytica-debacle-b69fe692d747>.

36 David Ingram, 'Facebook Nears Ad-Only Business Model as Game Revenue Falls', *Reuters* (online), 5 May 2018 <https://www.reuters.com/article/us-facebook-revenue/facebook-nears-ad-only-business-model-as-game-revenue-falls-idUSKBN1802U7>.

37 David Ingram, 'Exclusive: Facebook to put 1.5 Billion Users out of Reach of new EU Privacy Law', *Reuters* (online), 19 April 2018 <https://www.reuters.com/article/us-facebook-privacy-eu-exclusive/exclusive-facebook-to-put-1-5-billion-users-out-of-reach-of-new-eu-privacy-law-idUSKBN1HQ00P>.

The Federal Government's Bold Vision for Data Availability and Use

Partner Gavin Smith, Senior Associate Jessica Selby and Lawyer Claudia Hall consider the Federal Government's response to the Productivity Commission's report on data availability and use, released 1 May 2018.

Introduction

The Federal Government's response on 1 May 2018 to the Productivity Commission's report on Data Availability And Use (2017) (**PC Report**), outlines a bold vision but has a surprising lack of detail, suggesting implementation is likely to be some way off. If legislation is introduced, the new regime will result in a fundamental change to the way Australian consumers, businesses and government agencies interact with and think about data.

How does it affect you?

The Federal Government's Response has adopted most, if not all, of the recommendations in the Productivity Commission Inquiry Report on Data Availability and Use and confirmed the government's commitment to adopt a systems-wide approach to implementing an open data agenda. But it also leaves a huge amount of detail to be determined about the rights, obligations and governance framework under both the new Consumer Data Right (**CDR**) and data sharing and release (**DSR**) regimes.

The Response fails to replicate the PC Report's ambitious timeline for implementing the CDR and DSR regimes. The Federal Government has, historically, been slow to pass privacy legislation. Given the substantial amount of detail that remains to be determined, and a legislative road jam ahead of the next federal election (likely to be held in early 2019), we think it is unlikely that legislation codifying the CDR and DSR regime will be passed imminently.

If and when the government introduces legislation for the CDR and DSR regimes, there will be a ground-shift in the approach to data governance and valuation and the understanding of the utility of data in Australia. We predict the key impacts will be:

- **Private sector**
  - Businesses subject to the CDR will need to implement processes to identify what consumer data they hold and to enable consumers to access or transfer consumer data that is subject to the regime to themselves or third parties. Businesses in the banking, energy or telecommunications sectors should be on high alert, as the CDR will be introduced first to these sectors.
  - It is unclear whether the government intends to designate certain private sector datasets as, or as a component of, high-value datasets or Designated Datasets. If so, these private sector datasets might be required to be disclosed to, or compulsorily acquired by, government agencies or the broader market.
  - Once the Data Sharing and Release Act contemplated by the Response (**DSRA**) is introduced, businesses can apply to become a 'Trusted User' to obtain access to specified datasets that are not released to the public.
  - If the National Data Commissioner's functions include developing de-identification standards, businesses can consider whether they want NDC certification that they are using best practice de-identification processes and/or require that their service providers obtain such certification.
  - Businesses will likely be provided with greater access to searchable and comprehensive public-sector datasets.
- **Public sector**
  - Government agencies will need to implement processes (in conjunction with stakeholders) in relation to data sharing and management and de-identification.
  - Government agencies are likely to be required to disclose all information they hold that is not personal, commercial in confidence or 'particularly sensitive', for example because it relates to national security.
  - Depending on the scope of the DSRA, government agencies may have a greater right to access and require the release of information held by the private sector.
- **Consumers**
  - Consumers (and potentially small and medium enterprises (**SMEs**)) will have broader rights to access information about themselves in certain sectors, and the right to have that information transferred to a third party in order to improve their ability to make decisions about, and to acquire, products and services. The Response anticipates that the introduction of data portability will increase competition among service providers.
  - Individuals will be provided with greater access to searchable and comprehensive public datasets.[1]

1. Productivity Commission 2017, *Data Availability and Use*, Inquiry Report, Canberra, pages 33-52.

Background

- In May 2017, following public consultations and submissions on its draft report, the Productivity Commission released its Inquiry Report on Data Availability and Use, which included 41 recommendations. The PC Report was a landmark investigation on access and use of data in Australia, which criticised Australia's existing approach and proposed a need for 'fundamental and systematic change'. The PC Report set out an ambitious timeline that proposed all the recommendations be in place by 2020.
- In November 2017, the Federal Government announced that in 2018 it would bring forward legislation to create a Consumer Data Right (***CDR***) based on the PC Report recommendations. The announcement proposed the CDR would grant consumers across all sectors open access to their data, as well as an ability to direct a business to transfer their data to a third party in a usable machine readable form.
- In February 2018, the Federal Government released its Review into Open Banking, which included a new regulatory framework for 'Open Banking' (ie a framework for CDR for the banking sector).

Consumer Data Right

The Response accepts the PC Report's recommendation to introduce a CDR for the access and transfer of consumer data, administered by the Australian Competition and Consumer Commission (***ACCC***). The implementation of this recommendation was foreshadowed by the Federal Government's announcement in November 2017 and the recent Open Banking Review. The CDR will be rolled out progressively on a sector-by-sector basis, commencing with the banking, energy and telecommunications sectors and then moving to other sectors designated by the Treasurer.

Scope of the CDR

The Response provides that the CDR will empower consumers to:

- access particular data, such as transaction, usage and product data, in a useful digital format (***consumer data***); and
- transfer that data to themselves or third parties.

This is a more limited right than that set out in the PC Report, which also proposed allowing consumers to have the right to be informed of an entity's intention to disclose, exchange or sell data about that consumer for commercial gain.

Notably, the Response does not clarify whether the CDR is limited to individuals or whether it will extend to SMEs, although we note the Open Banking Review recommended that all consumers - that is individuals, small business *and* large business - be entitled to exercise the CDR, given the difficulties in delineating between small and large businesses.[2]

The PC Report provides that the type of consumer data required to achieve 'choice and competition benefits' under the CDR will be determined by government in consultation with the relevant sector and consumers. As with the remainder of the Response, this explanation lacks a lot of the detail contained in the PC Report, which proposed a wide definition of consumer data.[3] We believe the approach under the Open Banking Review is likely to be indicative of how the government will approach the CDR in practice for future sectors.[4] For example, the scope of consumer data under the Open Banking Regime is relatively limited being:

- digitally held customer-provided data (such as payee lists);
- data generated as a result of transactions made on a customer's account or service in relation to specified deposit and lending products; and
- product and service information that banks are already required to publicly disclose.[5]

The PC Report expressly excluded certain data from the scope of consumer data, for example, data subject to intellectual property rights or 'imputed data' about a consumer (ie data that has been created by the entity or a third party where it is merely probable that the characteristics are associated with an individual consumer).

The Open Banking Review excluded 'value-added data' (which results from material enhancement by the application of insights, analysis or transformation) from the scope of consumer data. This approach conflicts with the PC Report, which clearly distinguished between value-added data (data that has been made more useful) and imputed data, and proposed that value-added data *would* be considered consumer data and subject to the CDR.

The proposal that value-added data would be subject to the CDR was heavily criticised by the private sector (on the basis that it would reduce incentives to clean and organise data or invest in data analysis and transformation). We think it is unlikely, given the requirement to consult with sector groups, that the government will require that value-added data be subject to the CDR moving forward, and expect the government's ultimate approach will align more closely to the Open Banking Review's approach.

In addition, we predict that the implementation of the CDR in the

2. The Australian Government the Treasury 2017, *Review into Open Banking: giving customers choice, convenience confidence*, pages 41-42.
3. Productivity Commission 2017, *Data Availability and Use*, Inquiry Report, Canberra, page 207.
4. The Australian Government the Treasury 2017, *Review into Open Banking: giving customers choice, convenience confidence*, page vii.
5. Ibid, Recommendations 3.1 and 3.2.

energy and telecommunications sector will draw on the 'reciprocity' concept set out in the Open Banking Review. This approach could allow the government to ensure the CDR is adopted within the sector by mandating that the main telecommunication carriers, internet service providers and retail energy providers comply with the CDR, and requiring that any entities to whom telecommunications or energy consumer data is transferred under the CDR must provide *equivalent data* to consumers under the CDR regime.[6]

Governance

The CDR framework will consist of:

- legislative amendments to the *Competition and Consumer Act 2010* (Cth) (**CCA**), enabling the development of sector-specific binding rules by the ACCC in consultation with other relevant regulators; and
- sector-specific access, transfer, data and security standards to be developed by the new Data Standards Body in consultation with industry.

The Response contemplates that responsibility for overseeing the CDR will be split between the ACCC and the Office of the Australian Information Commissioner (**OAIC**).

The OAIC will be given responsibility for ensuring the CDR framework contains strong privacy protections[7] and for handling consumer complaints (with the justification that such complaints are likely to relate to privacy).[8]

The ACCC will have a significantly increased remit and will be responsible for:

- ensuring that the CDR system operates as intended and supports competition and consumer outcomes;
- investigating breaches and enforcing the CDR, including breaches that raise systemic competition issues, other than enforcement of privacy or confidentiality;
- determining the criteria for, and method of, accreditation for entities to whom consumer data can be transferred under the CDR; and
- potentially, monitoring and reviewing any costs reasonably incurred by entities in providing access to, or transferring, consumer data under the CDR.[9]

New Data Sharing and Release Regime

In addition to the new CDR system, the government has also proposed introducing a new legislative and policy regime to increase access to, and sharing of, data. The regime would apply in particular to public sector data. As with the CDR above, the Response does not clarify the details of the Data Sharing and Release Act or the roles of the National Data Commissioner (**NDC**) or Accredited Data Authorities (**ADAs**) (discussed below). In particular, the Response does not:

- clearly set out whether, or to what extent, the regime will apply to the private sector, although it appears to suggest that it might; or
- address the PC Report's recommendation that the government's template contracts be amended to include the right for government agencies to access or purchase the data under the contract.[10]

Data Sharing and Release Act

The Response proposes introducing a new Data Sharing and Release Act (**DSRA**) to underpin the data sharing and open access regime. In line with the PC Report, the Response suggests that the DSRA will be principles based and not overly prescriptive, suggesting that restrictions on use of or access to data be contained in contractual 'data use agreements' (discussed further under Accredited Data Authorities below).

The DSRA will:

- establish institutional and governance arrangements, including establishing an accreditation process and governance framework for ADAs and the 'Trusted User' framework; and
- set out rules and expectations around data sharing and release, and relevant safeguards for sensitive information (such as personal information, commercial in confidence information or information relating to national security).

The Response provides that the DSRA will not affect existing protections of particularly sensitive information (such as national security and law enforcement data) or secrecy provisions in relation to identifiable information. This expressly rejects the approach put forward in the PC Report, that the DSRA might authorise the sharing and releasing of data *despite* the provisions of other legislation, such as privacy legislation.

National Data Commissioner

The NDC will be established as an independent statutory authority. The Response indicates that the NDC's functions will be to monitor the integrity of and oversee the DSR regime and the DSRA, in particular the data sharing and release activities of Commonwealth agencies, and to provide guidance on technical best practice and ethical access to and use of data.

The scope of the National Data Commissioner's remit is not clearly expressed in the Response. The PC Report suggested that the National

6. Ibid, Recommendation 3.9.
7. Ibid, page 18.
8. Ibid, page 17.
9. Productivity Commission 2017, *Data Availability and Use*, Inquiry Report, Canberra, page 19.
10. Ibid, Recommendation 6.3; Ibid, page 241.

Data Commissioner be given broad scope to deal with both private and public sector access to, and sharing or release of, data. However, the Response repeatedly refers to *public data* and the *government's* use or management of data. This suggests to us that the NDC's remit might in fact be limited to the administration of the DSR regime *only* in respect of the public sector. This leads to a broader question about whether the government intends for the DSR and 'open access' regime to govern the private sector, as recommended in the PC Report.

It is not clear whether the NDC's functions will also include additional activities that were set out in the PC Report, for example:

- developing standards for the de-identification of data and guidance on re-identification risks;[11]
- developing guidance on how to manage risks in sharing identifiable data between entities;[12] or
- setting prices for organisations to access datasets.

The Response further provides that the NDC will receive guidance from the Australian Bureau of Statistics (**ABS**) in respect of technical issues, and a new National Data Advisory Council in respect of ethical data use, technical best practice and industry and international developments.

Accredited Data Authorities

The Response commits to accrediting bodies with particular expertise as Accredited Data Authorities. The Response provides that the accreditation and governance process for ADAs will be similar to that for ABS and the Australian Institute for Health and Welfare as 'Integrating Authorities'. Accordingly, it is likely that each ADA will be a Federal Government agency, or otherwise a 'secure and trusted institution' bound by the *Privacy Act 1988* (Cth), and that they will have sole responsibility for administration and management of a number of datasets, including the provision of access to relevant Trusted Users (discussed further below).

As set out in the Response, two of the ADAs' key responsibilities will be:

- determining whether a dataset is made available for public release or otherwise for limited sharing with Trusted Users; and
- entering into data use agreements with Trusted Users, data custodians and data users. These agreements will outline the conditions of, and restrictions on, access to data, risk management arrangements, as well as permitted actions in respect of the shared data (for example, integration of the dataset with other data or release of a non-sensitive version of the dataset).[13]

Trusted Users

The PC Report contemplated that Trusted Users would be individuals who are approved by an ARA to access and use data that is sensitive or is otherwise not publicly available. The Response does not clarify the government's approach to Trusted Users, apart from acknowledging that it will be based on the UK 'five safes' model. While the Response does not specify who might be entitled to be a Trusted User, we believe it is likely to consist of the entities identified in the PC Report, namely government agencies, universities, not-for-profits, corporates and research bodies (where bound by the Privacy Act).

We expect that Trusted Users will be classified on a scalable basis, with the level of trust the user has influencing the accreditation, reporting and compliance requirements. While private sector entities may be entitled to become Trusted Users, they are likely to be subjected to more stringent access and use restrictions, including controls on accessing potentially identifiable data about businesses in the same industry.

Designated Datasets – a special class of high-value datasets

In the Response, the government agreed to establish a framework to identify 'Designated Datasets' (***DDs***), being datasets whose availability and use would generate significant community-wide benefits. The Response classifies DDs as a 'special class of high-value datasets' whose release would complement work done about high-value datasets under the *Open Government Partnership National Action Plan 2016-2018* (**Action Plan**). Given that high-value datasets under the Action Plan only relate to public sector data, we think this suggests that DDs might similarly be limited to public sector datasets.

This approach would be at odds with the PC Report, which suggested that there could be situations where there is a national interest in including private sector information in a DD, such as data held and collected due to services funded or legislatively authorised by Commonwealth or State public policy (eg data held by banks, health insurance funds and energy providers).[14] This recommendation in the PC Report received negative backlash from the private sector, so it is possible that the government has reduced the scope of DDs such that they will only contain public sector data, or that the government has left the Response intentionally vague to give itself more time to determine whether it requires private sector DDs.

The government has also committed to publishing a register of available publicly-funded datasets and giving priority to the release, curation and streamlining of access to datasets

11. Ibid, page 320.
12. Ibid, Recommendation 8.2.
13. Ibid, Recommendations 6.9 and 8.3; Ibid, pages 269, 322.
14. Ibid, pages 305-306.

with the greatest potential to deliver social and economic outcomes for the country.[15]

Looking forward

The open access approach championed by the Productivity Commission and supported by the Federal Government's Response signifies a fundamental change in the attitude to the access and use of data in Australia.

The PC Report and the Government's Response propose a framework that will dramatically shift the way in which data is thought about and managed by government, the private sector and individuals. While greater access to public and private datasets is likely to improve the insights that can be gained about population trends and may improve the setting of public policy, it is also likely to impose a cost on private entities, both in relation to compliance and through increased levels of competition. It will increase the potential risk for data to be misused. It remains to be seen whether the government in weighing these costs has determined that they will only implement the open data framework and DSR regime in respect of the public sector.

Crucially, in attempting to implement the new DSR and CDR regimes, the government must ensure that data is provided in a meaningful and understandable way to consumers and the broader public and is not released in quantities that are overwhelming, and that personal and commercial-in-confidence information is protected.

The Response leaves all details of the proposed regime open to be determined. The proposed regime will need to be implemented through the drafting of the amending legislation to the CCA, the DSRA and through guidance issued by the NDC, ACCC and the Data Standards Body. Given that the NDC has not yet been established and legislation has not yet been put forward, it is unlikely that the new DSR and CDR regimes will be implemented until at least next year.

While big changes to Australia's privacy and data landscape appear to be on the horizon, until the detail and enabling legislation is settled, it is not possible to say with certainty what this brave new world will look like for the Australian public and private sector.

15. Commonwealth of Australia, Department of Prime Minister and Cabinet 2016, *Australia's First Open Government National Action Plan 2016-2018*, page 25.

Michelle Rowland MP:

Old media, new media, not media:

Rethinking policy for the public interest

"We need a coherent, principled and evidence-based approach to guide a transition where all players do their bit"

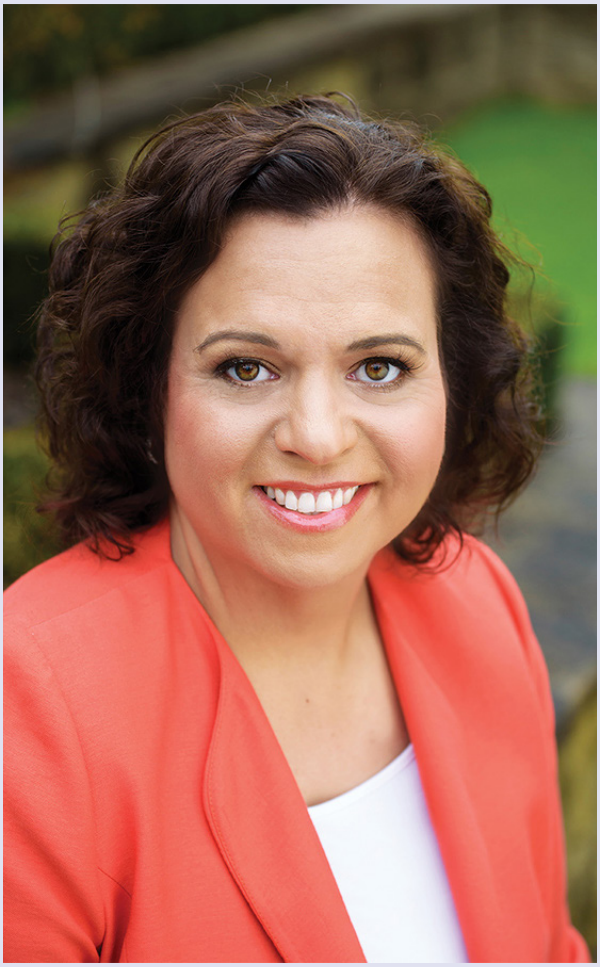
With recent developments in policy and regulation suggesting that Australia is barely playing catch-up, Michelle Rowland MP, Shadow Minister for Communications will provide a presentation on the role of Government in promoting public interest objectives and the need to adapt as the media ecosystem evolves.

To encourage openness and the sharing of information for the benefit of its members, unless specified otherwise, all CAMLA events are subject to the "Chatham House Rule" which provides that participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.

Date and Time
17 May 2018
Registration: 5.45pm
Seminar: 6.00-7.00pm
Drinks and canapés: 7.00-9.00pm

Venue
Gilbert + Tobin
Level 35, Tower Two,
International Towers
200 Barangaroo Avenue
Barangaroo, NSW

Cost
$70 for members
$95 for non-members



CAMLA Young Lawyers Networking Event and Essay Competition

On Wednesday evening, 14 March 2018 CAMLA held its Young Lawyers Networking event at the offices of King & Wood Mallesons. The event was proudly organised by the CAMLA Young Lawyers Committee. The event provided an excellent opportunity for young lawyers and law students to gain valuable insights into a number of career paths within both the media and communications industries from a panel of accomplished and inspiring professionals.

This year, the diverse and very experienced panel consisted of Cate Nagy (Partner at King & Wood Mallesons), Matthew Lewis (Barrister at 5 Wentworth Chambers), Johnathan Carter (Head of Legal, Corporate and Policy at APRA AMCOS) and Kirsty McLeod (Senior Corporate Counsel at Channel Ten). The event was chaired by Maggie Chan, Senior Associate at King & Wood Mallesons. The panel candidly recounted some of their war stories and the highlights of their career with the audience. They also provided some insightful lessons and career tips to the audience, comprising of the following:

- first impressions are imperative.
- networking is important, both internally within the business and externally.
- where you start your career isn't where you will necessarily end up.
- the need to have a genuine interest in the law.
- be authentic in your interests.
- show initiative.

The event also provided an opportunity for networking at the conclusion of the panel presentation and the opportunity to announce and celebrate the winners of CAMLA's annual essay writing competition.

Awards were presented to Penelope Bristow of the University of Queensland for her essay, "#Trending – The Rise of Social Media and the Challenges for Australia's Defamation Law", Claudia Carr of Curtin University on her essay on Net Neutrality in Australia and Anna Belgiorno-Nettis of Gilbert + Tobin on her essay on the topic of 'Does the Broadcasting Reform Act give up on democracy?' The first two of those essays are published in this edition of the *Communications Law Bulletin*. The third is forthcoming.

Report by Stef Russo, Legal Counsel at IRESS Limited.

GDPR: The Final Countdown
What it Means for Australia

Veronica Scott, Special Counsel, and Ashleigh Fehrenbach, Associate, at MinterEllison, describe how the GDPR impacts Australian businesses, particularly in the media sector.

From 25 May 2018, the General Data Protection Regulation (2016/679) (**GDPR**) is set to replace the current EU data protection regime as the new European Data Protection law. Its purpose is to protect fundamental rights and freedoms of individuals when processing their personal data (wherever that may happen) and enable the free movement of personal data within the European Union (**EU**).

Due to the broad extra-territorial provisions in Article 3 of the GDPR, Australian businesses of any size (including media companies) may need to comply with the GDPR if they have an establishment in the EU, or if they do business in Europe by offering goods and services to individuals in the EU, or if they monitor the behaviours of individuals that takes place in the EU. The GDPR will take direct effect in all member states of the Union and in countries in the broader European Economic Area (**EEA**). The obligations that businesses will have will depend on whether they are a data controller or data processor.

The GDPR will apply in the UK at least until Brexit occurs (which will not be until at least 2019). The GDPR includes many obligations and rights that are similar to those in the Privacy Act and is founded on seven key data protection principles, with similar objectives to the APPs - to foster transparent information handling practices and business accountability in relation to data processing and handling. However, there are also additional stricter measures and individual rights in the GDPR. The GDPR also has hefty fines which gives it much sharper teeth than the Privacy Act.

Many of the requirements in the GDPR align with the steps that the Office of the Australian Information Commissioner (**OAIC**) expects Australian APP entities to take (as outlined in particular in the OAIC's Guidelines to the APPs), but which are not necessarily strictly required by the APPs. This is a reflection of the fact that the Privacy Act is broadly all principles based law, whilst the GDPR is highly prescriptive. It also includes additional rights for individuals. In short, best practice compliance with the APPs will support (but not ensure) compliance with the GDPR.

The GDPR has generated much discussion throughout the hallways of Australian law firms, as well as on a global level and is set to change the global privacy landscape for good raising the bar for data protection. The general view is that Australian businesses with a global focus should be asking:

(a) whether and to what extent they will be required to comply with the GDPR as a data controller or processor;

(b) assuming they need to comply, do any exemptions apply;

(c) what kind of steps do they need to take to achieve compliance as a controller or processor (ie those that are additional to the requirements in the Australian Privacy Principles (**APPs**) in the *Privacy Act 1988 (Cth)* (**Privacy Act**)); and

if they don't, what are the risks and potential regulatory consequences.

So, when does it apply?

The extra-territorial provisions in Article 3 of the GDPR extend its scope to the 'processing' of 'personal data' of data subjects (natural individuals) who are in the EU by a 'data controller' who is not established in the EU, where the processing activities relate to:

(a) offering the data subjects goods or services, irrespective of whether they are required to pay; or

(b) monitoring their behaviour as far as their behaviour takes place within the EU.

The definition of 'personal data' is similar to the Australian definition of personal information but specifically includes data such as identifiers. The act of 'processing' of their personal data covers all the acts and practices that are performed on it during its lifecycle, whether automated or not. It includes collection, recording, retrieval, use, storage, combining, automated processes and disclosure by transmission.

A 'data controller' includes the natural or legal person or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Data controllers have the most direct and onerous obligations under the GDPR. A 'data processor' processes personal data on the instruction of the controller (eg through a contract).

Despite these seemingly simple definitions, it is important to understand that assessments of whether or not the GDPR will apply to Australian businesses processing personal data about data subjects in the UK or other countries in the EEA are extremely fact sensitive.

Key additional requirements in the GDPR

We have outlined below the key gaps between the APPs and GDPR requirements and the main factors

that will need to be considered by media organisations in order to comply with these requirements.

Right to privacy enshrined

The GDPR gives Member States the ability to make laws in relation to some aspects of data processing. In particular for media organisations, Article 85 provides that Member States need to reconcile the right to privacy with the freedom of expression (both rights enshrined in the *European Union Charter of Fundamental Rights* (articles 8 and 10), when the processing of personal data is for purposes of, in particular, journalism, and in so far as this is necessary for the fundamental right to receive and impart information. This is a relatively vague provision and the only certainty the GDPR has provided is contained in Recital 153 "*This should apply in particular to the processing of personal data in the audiovisual field and in news archives and press libraries.*" and *"it is necessary to interpret notions relating to that freedom, such as journalism, broadly*."

Appoint a representative in the EU[1]*:* If an Australian business does not have an establishment in the EU, it will be required to appoint a representative established in an EU member state if its data processing meets certain thresholds. The role of the representative is to be a point of contact for supervisory authorities and individuals in the EU on all issues that relate to data processing, in order to ensure compliance with the GDPR.

Appoint a data protection officer ***(DPO)***[2]*:* Some data controllers will be required to designate and give resources to a DPO, which is an independent, expert and protected role, to monitor and advise on internal compliance with the GDPR and be accessible to data subjects and supervisory authorities.

Accountability - demonstrate compliance[3]*:* Not only must businesses comply, they must be able to **demonstrate** compliance with the data protection principles in the GDPR. (These apply to the handling of the personal data across its entire lifecycle, and are very similar to the APPs):

(a) Personal data must be processed lawfully, fairly and in a transparent manner;

(b) Purpose limitation - personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (with exceptions for public interest, scientific, historical or statistical purposes);

(c) Data minimisation - personal data must be adequate, relevant and limited to what is necessary in relation to purposes for which it is processed;

(d) Accuracy - personal data must be accurate and, where necessary, kept up to date. Inaccurate personal data should be corrected or deleted;

(e) Retention - personal data should be kept in an identifiable format for no longer than is necessary (with exceptions for public interest, scientific, historical or statistical purposes); and

(f) Integrity and confidentiality - personal data must be processed in a manner that ensures its security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Lawful basis for processing: Business will be required to demonstrate that they can rely on one of the following applicable lawful bases for processing personal data:

- Necessary to perform a contract or at the request of the individual before entering the contract
- Consent
- Necessary to comply with the business's legal obligations
- Necessary for the legitimate interests of the business or a third party which don't override the individual's interests
- Secondary purposes compatible with the primary purpose of collection

Privacy *by design and by default*[4]*:* the GDPR reflects a risk based approach to data protection (with similarities to the reasonable steps approach in the APPs). Businesses are required to implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to support the Data Protection Principles, taking into account the nature, scope, context and purpose of the processing.

*Undertake data protection impact statements (****DPIAs****)*[5] *and consult with supervisory authority about high risk processing*[6]: Businesses will be required to undertake a DPIA where a type of processing is **likely to result in a high risk** to the rights and freedom of individuals and, if this is indicated by the DPIA (in the absence of risk mitigation measures), consult with a supervisory authority before undertaking the processing

1 Article 27
2 Article 37
3 Article 5 (2)
4 Article 24
5 Article 35
6 Article 36

which can issue advice, request further information or give a warning. DPIAs are similar to what are known as privacy impact assessments in Australia (which the OAIC considers should be undertaken in certain circumstances as a reasonable step to comply with APP 1). However, consistent with its more prescriptive approach to compliance, the GDPR mandates these.

Expanded rights for individuals[7]: The GDPR strengthens the rights of individuals and affords them new rights, in particular in relation to the right to be forgotten[8], the right to data portability[9], the right to object to processing[10] and the right not to be subject to a decision based only on automated processing[11].

The right to be forgotten requires businesses to delete (erase) personal data on request from the data subject (subject to certain exceptions). Data may also need to be deleted if it cannot be processed in accordance with the GDPR. If the data has been published to other data controllers, reasonable steps must be taken to inform the other controllers of the requirement for erasure. This highlights the importance of keeping records of disclosure.

The right to data portability has two aspects. First it requires (on request) the provision to the data subject of his or her personal data in a structured, commonly used and machine readable format. The second, and arguably more onerous requirement, is to transfer an individual's personal data to another controller on request.

The right to object relates to objecting to specific types of information processing including, for example:

(a) direct marketing;

(b) processing based on legitimate interests or performance of a task in the public interest/ exercise of official authority; and

(c) processing for research or statistical purposes.

The right not to be subject to a decision based on automated processing is a right to avoid being '*subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning [the data subject] or similarly significantly affects [the data subject].*' Recital 58 provides as examples the '*automatic refusal of an on-line credit application or e-recruiting practices without any human intervention.*' There are some exceptions to this right that permit the automated processing.

Different data breach notification requirements[12]: The requirements are similar to Australia's mandatory breach notification requirements[13] but there are some key differences, including lower thresholds and tighter deadline for reporting to the relevant supervisory authority. Reporting of a data breach must happen within **72 hours** of becoming aware of the breach, unless that breach is unlikely to result in 'risk to the rights and freedoms' of individuals (this threshold of "risk" is potentially a lower threshold to "serious harm" in the Australian laws).

Stricter consent requirements[14]: If a business requires consent for any processing of personal data, (eg direct marketing or for lawful processing), it will need to comply with very strict requirements to establish valid consent. Consent must be freely given, specific, informed and an unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify agreement to the particular processing.

For the most part the consent requirements under the GDPR reflect the elements of valid consent as set out in the APP Guidelines. However there are further specific requirements under the GDPR including that a business would need to inform individuals about the right to withdraw consent, it must be demonstrable, distinguishable and based on clear affirmative action or statement.

Consent to processing of health data[15]: Australian business will require *explicit* consent to process sensitive personal data (noting that processing covers the handling of the personal data across its entire lifecycle, not just the initial collection). This entails a degree of formality, for example the individual ticking a box containing the express word "consent". Explicit consent cannot be obtained through a course of conduct.

Transparency[16]*:* Australian business will be required to give individuals a range of prescribed information about the processing of their personal data. This information must be concise, transparent, intelligible

7 Articles 15 to 22
8 Article 17
9 Article 20
10 Article 21
11 Articles 21 and 22
12 Article 33
13 *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth)
14 Article 4 (11)
15 Article 9 (2)
16 Articles 12, 13 and 14
17 Article 28

and easily accessible using clear and plain language (reflecting what the OAIC expects of Australian notices). This is similar to an APP 5 collection notice, but the GDPR requires additional information about express retention periods, the data subject's rights and, if there are overseas transfers, what safeguards are in place to permit overseas transfers.

Contracts with service providers (data processors)[17]*:* If a data controller engages a service provider who will be processing the personal data of data subjects in the EEA on behalf of the controller, it needs to use only processors who can provide sufficient guarantees in relation to safeguarding the data and ensure there is a written contract with the data processor that includes specific provisions as set out in the GDPR. Whilst current or template contracts may contain some of these clauses (e.g data security, use limitation, breach notification) businesses will need to impose more prescriptive requirements on processors. These include acting only within the scope of written authority of the controller.

Overseas transfers[18]: Unlike APP 8, the GDPR only permits the transfer of personal data outside the EEA (and onwards to another country outside the EEA) in certain prescribed circumstances, although some of the permitted circumstances are similar to the exception to the APP 8.1 reasonable steps obligation. These permitted circumstances are: transfers to countries with an "adequacy finding", transfers based on appropriate safeguards (through standard model clauses) or binding corporate roles. There are some other limited derogations, such as consent, but they have strict requirement.

Tougher sanctions[19]: The GDPR has high sanctions for non-compliance. For many breaches, supervisory authorities will be able to issue fines of up to 4% of annual worldwide turnover or €20 million. For breaches of other GDPR requirements, the fines can be up to 2% of annual worldwide turnover or €10 million. They also have a wide range of other powers such as broad investigatory powers and the powers to issue reprimands, impose a temporary or definitive limitation (including a ban) on processing, and impose administrative fines.

It will be interesting to see how the exceptions in Article 85 will be implemented. It is clear however that Australian media organisations who operate in Europe will need to carefully consider the impact of the GDPR, understand the personal data they hold about relevant individuals, how it is processed and the gaps in compliance.

Veronica Scott is a Special Counsel, and **Ashleigh Fehrenbach** is an Associate, at MinterEllison. Ashleigh is also a member of the CAMLA Young Lawyers Committee.

18 Article 45
19 Article 83 (5)

#Trending: The Rise of Social Media and the Challenges for Australia's Defamation Law

Penelope Bristow, finalist in the 2018 CAMLA Young Lawyers Essay Competition, provides an overview of the application of defamation law in the context of social media.

I Introduction

Social media has changed the way we communicate, and is now used by around 80% of people in Australia.[1] The rise of social media has been accompanied by an increase in the number of online defamation cases.[2] Australia's defamation laws are struggling to keep pace. This is because social media platforms are fundamentally different from previous forms of media and internet publishing: content is primarily created by individual users and there is no editorial 'filter' between the creator and publication.[3] Further, the information posted to social media can be scrutinised, searched and broadly disseminated without the original poster's knowledge or consent.[4]

However, people still tend to view social networking sites as virtual venues rather than as publications.[5] This perception is apt to mislead, as summarised by Kenneth Martin J in *Douglas v McLernon (No 4)*:[6]

> There still manifests a perception in some members of the community that the laws of defamation do not apply to publications made over the internet. Consequently, there is a lingering misapprehension that anything at all can be posted concerning another person over the internet no matter how defamatory or scandalous the uploaded material may be and that the posted material will enjoy a complete immunity. That perception is wrong…

Although it is clear that defamation law applies to social media, the novel and evolving nature of such platforms presents a number of issues. What amounts to publication online? When is defamatory material considered to be published online? How should damages be assessed in online defamation cases? Indeed, the application of existing defamation law to publications made on social media is often inadequate and unsatisfactory. Although there have been calls for reform,[7] little progress has been made to enact change.

II Brief Overview of Australia's Defamation Law

The purpose of defamation law is to vindicate and protect against reputational damage.[8] To be liable for defamation requires the publication of material which is likely to lower the plaintiff in the eyes of a reasonable member of the community.[9] Publication may occur by way of a positive act, or by omission.[10] Publication by a positive act requires the defendant to intentionally assist in the publication of the defamatory material.[11] In the context of social media, publication by positive act may include posting or commenting on Facebook,[12] posting or commenting on LinkedIn,[13] or tweeting on Twitter.[14] Publication by omission requires the defendant to have impliedly ratified or adopted the defamatory material through inaction.[15] In the context of social media, a 'secondary publisher' may include the administrator of a Facebook page,[16] or a search engine.[17]

1 Sensis, *Sensis Social Media Report 2017* (June 2017) 3.

2 Judith Gibson DCJ, 'From McLibel to e-Libel: Recent issues and recurrent problems in defamation law' (Paper presented at the State Legal Convention, New South Wales, 30 March 2015); Walter MacCallum, 'Defamation actions and social media: Where are the risks?' (2015) 67 *Governance Directions* 677, 677. See also *Rothe v Scott (No 4)* [2016] NSWDC 160, [141] (Gibson DCJ).

3 Jennifer Ireland, 'Defamation 2.0: Facebook and Twitter' (2012) 17 *Media and Arts Law Review* 53, 54.

4 Ibid.

5 Patrick Lim, 'You have 3 friend requests and 1 criminal conviction: tackling defamation on Facebook' [2010] (3) *Internet Law Bulletin* 169, 170.

6 [2016] WASC 320, [1].

7 See, eg, Communications Alliance Ltd, Submission to the Attorney General, *Review of the Defamation Act 2005*, 5 May 2011; Joint Media Organisations, Submission to the Attorney General, *Review of the Defamation Act 2005*, 25 February 2016.

8 David Rolph, *Defamation Law* (Thomson Reuter, 2016) 600, 606-607; Ryan Turner, 'Internet defamation law and publication by omission: a multi-jurisdictional analysis' (2014) 37(1) *UNSW Law Journal* 34, 40.

9 *Sim v Stretch* [1936] 2 All ER 1237.

10 *Frawley v New South Wales* [2007] NSWSC 1379, [8]-[9] (Berman AJ).

11 *Webb v Bloch* (1928) 41 CLR 331, 364 (Isaacs J).

12 See, eg, *Dabrowski v Greeuw* [2014] WADC 175; *Mickle v Farley* [2013] NSWDC 295; *Polias v Ryall* [2014] NSWSC 1692.

13 See, eg, *Jeffrey v Giles* [2013] VSC 268.

14 See, eg, *Lord McAlpine v Bercow* [2013] EWHC 1342; *Cairns v Modi* [2010] EWHC 2859.

15 *Frawley v New South Wales* [2007] NSWSC 1379, [17] (Simpson J).

16 See, eg, *Von Marburg v Aldred* [2015] VSC 467; *Murray v Wishart* [2014] 3 NZLR 722.

17 *Google Inc v Duffy* [2017] SASCFC 130.

III Issues in Applying Existing Defamation Law to Social Media

A. Trying to Fit a Square Archaic Peg into the Hexagonal Hole of Modernity:

What Amounts to 'Publication' Online?

The concept of publication is especially vulnerable to disruption by social media.[18] Indeed, '[t]he rapid expansion of the internet coupled with the surging popularity of social networking services like Facebook and Twitter have created a situation where everyone is a potential publisher.'[19] Existing defamation law has not delivered entirely satisfactory conclusions. Take, for example, the posting of hyperlinks and the hosting of webpages.

1. *Posting a Hyperlink to Defamatory Material*

Hyperlinks are ubiquitous on the internet: they appear in articles, blogs, social media, advertising, and search engine results. On social media, users often post or share links to other websites or online articles. Without hyperlinks, 'the web would be like a library without a catalogue; full of information, but with no sure means of finding it'.[20] However, hyperlinks also facilitate the spread of defamatory material.[21] Can a hyperlink be said to 'publish' the material it connects to?

Australian courts have not yet considered whether hyperlinks 'publish' material. The Supreme Court of Canada in *Crookes v Newton* held that '[a] hyperlink, by itself, should never be seen as publication of the content to which it refers, even if the hyperlink is followed and the defamatory content is accessed'.[22] This conclusion was supported by the fact that the defendant had no control over the content capable of being accessed through the hyperlink. An exception was recognised where the defamatory material was repeated in the hyperlink text itself.

Importantly, however, the decision represented a departure from existing Canadian defamation law. Traditionally, the form of publication was irrelevant:[23] any act which had the effect of transferring the defamatory material to a third person was sufficient.[24] In coming to its decision, the majority acknowledged that a strict application of this rule would be like 'trying to fit a square archaic peg into the hexagonal hole of modernity'.[25] Certainly, the same could be said for other areas of defamation law when applied to social media, and Australian courts should feel emboldened to mould our defamation law to better deal with the challenges thrown up by social media.

In any event, it will be difficult to fashion a 'one-size-fits-all' approach to hyperlinks, due to their functional diversity. For example, even if the decision in *Crookes v Newton* is taken as a guide, it was confined to user-activated hyperlinks and did not consider the approach to take to embedded or automatic hyperlinks. This complexity creates unavoidable challenges for legal uniformity.

2. *Hosting a Page on which Defamatory Material is Posted*

Suing individuals who post defamatory material to a social media page may be futile due to the anonymity of the internet and the difficulty of enforcing an award.[26] A more lucrative and attractive option is to sue the host of the social media page, which may be a large corporation.[27] As a result:

> The unity between legal responsibility and moral fault for the publication of defamatory material may diverge as claimants pursue litigation against corporate entities with peripheral engagement in the act of publication rather than the primary or direct publisher.[28]

In *Von Marburg v Aldred*,[29] the plaintiff submitted that the administrator of a Facebook page could be said to have 'published' posts and comments made to that page by other Facebook users. In the preliminary hearing, Dixon J set out a number of relevant principles. His Honour held that to allege that the host of a Facebook page is a primary publisher of defamatory material on that page, the plaintiff must show that the host was either instrumental in the act of publication, or that the host had the ability to control whether publication occurred. Alternatively, to allege that the host of a Facebook page is a secondary publisher, the plaintiff must show that the host:

(i) acquired knowledge of the existence of the impugned publication;

(ii) had sufficient responsibility for the content of the Facebook page, whether as owner, sponsor, administrator or moderator to exert control over its content; and

18 Stephanie Rigg, 'The Duke and his manservant in a world of online defamation: Rethinking the multiple publication rule in 21st century Australia' (2016) 21 *Media and Arts Law Review* 424, 424.

19 *Crookes v Newton* [2011] 3 SCR 269, [38] (Abella J).

20 Ibid, [34] (Abella J).

21 Ibid, [105] (Deschamps J).

22 *Crookes v Newton* [2011] 3 SCR 269, [44] (Abella J).

23 Ibid, [16] (Abella J).

24 *Stanley v Shaw*, 2006 BCCA 467, 231 B.C.A.C. 186.

25 *Crookes v Newton* [2011] 3 SCR 269, [36] (Abella J).

26 Turner, above n 5, 61.

27 MacCallum, above n 2, 678.

28 Turner, above n 5, 40.

29 [2015] VSC 467. See also *Murray v Wishart* [2014] 3 NZLR 722.

(iii) failed to remove the communication in circumstances which support the conclusion that the host is responsible for, or has ratified, the continuing publication of that communication.

This treatment of internet intermediaries has the potential to widen the divergence between legal responsibility and moral fault for the publication of defamatory material. This divergence was acknowledged by submissions made to the 2010 review of the *Defamation Act 2005* (NSW). Many media organisations raised the need for a 'safe harbour' provision to provide certainty to online intermediaries as to their liability for defamatory material produced by third party content providers.[30] Seven years later the issue is still a live one and little progress has been made. As observed by Kourakis CJ in *Google Inc v Duffy*:

> The degree of control which is sufficient to attract liability will continue to arise in relation to other social media platforms like Facebook, Twitter and Instagram. The related public policy question of the degree to which the managers of those platforms should be given, and exercise, censorial responsibility over content based on their judgment as to what is defamatory… will also continue to throw up difficult issues.[31]

B. Continuous and Perpetual Publication Online:

When is Defamatory Material Considered to be Published?

Currently, each jurisdiction in Australia has a limitation period of one year, running from the date of publication.[32] The 'multiple publication rule' provides that each communication of defamatory material amounts to a separate publication: each time the material is published a new cause of action accrues and a new limitation period begins to run.[33]

In *Dow Jones & Co Inc v Gutnick*,[34] the High Court of Australia held that every time a webpage containing defamatory material is accessed, a new cause of action accrues against the publisher.[35] As a consequence, 'the limitation period [for online defamation] is effectively open-ended, with a fresh limitation period starting to run each and every time defamatory material is accessed online.'[36] In this way, the one year limitation period can be extended indefinitely by showing that the relevant content has been accessed within the preceding twelve months. In the context of social media, a single like, share, favourite, or re-tweet may be sufficient to 'reset' the clock.

Consequently, the continued application of the 'multiple publication rule' to online publications, including posts made to social media, casts an unacceptably wide net of potential liability.[37] The generosity that the rule bestows upon plaintiffs is accompanied by a correspondingly significant burden on social media users.[38] This is because the multiple publication rule allows for the possibility of 'continuous' or 'perpetual' publication in online archives.[39] For this reason, there have been calls to adopt a 'single publication rule' in Australia,[40] similar to that adopted in the United Kingdom,[41] or the United States.[42] Again, this issue demonstrates the problems associated with the application of existing defamation law to social media.

C. Their Evil Lies in the Grapevine Effect:

How should Damages be Assessed in Online Defamation Cases?

Damages awarded for defamation serve three purposes: 'consolation for the personal distress and hurt caused to the appellant by the publication, reparation for the harm done to the appellant's personal and (if relevant) business reputation and vindication of the appellant's reputation.'[43] The quantum of damages should reflect the injury to the plaintiff's reputation.[44] If defamatory matter emerges from its lurking place at some future date, the plaintiff must be able to point to a sum awarded as sufficient enough to convince a bystander of the baselessness of the charge.[45]

30 See, eg, Communications Alliance Ltd, Submission to the Attorney General, *Review of the Defamation Act*, 5 May 2011, 3; Joint Media Organisations, Submission to the Attorney General, *Review of the Defamation Act 2005*, 25 February 2016, 2.

31 [2017] SASCFC 130, [149].

32 See, eg, *Limitation Act 1969* (NSW) s 14B; *Limitation of Actions Act 1974* (Qld) s 10AA; *Limitation of Actions Act 1936* (SA) s 37; *Limitation Act 2005* (WA) s 15; *Limitation of Actions Act 1958* (Vic) s 23B.

33 *Duke of Brunswick v Harmer* (1849) 117 ER 75; *R v Carlisle* (1819) 1 Chit 451, 453.

34 (2002) 210 CLR 575.

35 *Dow Jones & Co Inc v Gutnick* (2002) 210 CLR 575, [44] (Gleeson CJ, McHugh, Gummow and Hayne JJ)

36 Anne Flahvin, 'The Future of the 'Multiple Publication' Rule' (2009) 28(2) *Communications Law Bulletin* 13, 13.

37 Rigg, above n 24, 425.

38 Itai Maytal, 'Libel Lessons from Across the Pond: What British Courts Can Learn from the United States (2010) 3 *Journal of International Media & Entertainment Law* 121, 123, quoting Patrick Milmo and WVH Rogers (eds), *Gatley on Libel and Slander* (Sweet & Maxwell, 10th ed, 2004) 6.2.

39 Ireland, above n 20, 66.

40 See, eg, Communications Alliance Ltd, Submission to the Attorney General, *Review of the Defamation Act*, 5 May 2011, 3; Joint Media Organisations, Submission to the Attorney General, *Review of the Defamation Act 2005*, 25 February 2016, 2. See also Matthew Collins, 'Five years on: A report card on Australia's national scheme defamation laws' (2011) *Media and Arts Law Review* 317, 339.

41 *Defamation Act 2013* (UK) s 8.

42 *Wolfson v Syracuse Newspapers Inc* 254 App. Div. 211 (1938); *Firth v State* 98 N.Y.2d 365.

43 *Carson v John Fairfax and Sons Ltd* (1993) 178 CLR 44.

44 Uren v John Fairfax & Sons Pty Ltd (1966) 117 CLR 118, 151 (Windeyer J); *Corneo v Kurri Kurri and South Maitland Amusement Co Ltd* (1934) 51 CLR 328, 343 (Rich, Evatt and McTiernan JJ).

The assessment of damages in defamation cases involving social media is particularly difficult. Defamatory publications on social media have an increased capacity to spread, or re-surface at some later date: 'their evil lies in the grapevine effect.'[46] The grapevine effect is 'the realistic recognition by the law that, by the ordinary function of human nature, the dissemination of defamatory material is rarely confined to those to whom the matter is immediately published.'[47] Certainly, the dissemination of defamatory material on social media is now devastatingly quick and easy. The defamatory material can be shared to hundreds or thousands of other users with the click of a button, and can be re-discovered and re-posted later due to the internet's vast memory.

In assessing damages in social media defamation cases, Australian courts have taken divergent approaches, particularly when considering the implications of the size and reach of the internet. One approach appears to be that the sheer number of social media pages militates against an inference that defamatory material has been viewed by anyone at all. This was the approach taken in *Sims v Jooste [No 2]*,[48] where Martin CJ at [17] opined that:

> Because of the vast number of internet sites, and the vast number of web pages accessible through those internet sites, in the absence of evidence it cannot be inferred that one or more persons has undertaken the steps required to identify and access any particular web page available through the internet merely from the fact that material has been posted on an internet site.

A more common approach taken by the courts is to conclude that the grapevine effect is greater on social media, due to the ease and speed with which users can share and re-post information.[49] Indeed, for these reasons, courts have on some occasions inferred a greater readership of defamatory material than could be proven on the facts.[50] However, on other occasions, the confined readership of a post (e.g. to family and friends) has been held to increase the plaintiff's hurt and distress, compared to if the post had been shared with strangers.[51] These opposing approaches create uncertainty, and it is clear that a uniform approach is required.

V Future Challenges

Although Australia's current defamation law is ill-equipped to adequately deal with the issues caused by social media, reform presents its own challenges. The internet has been recognised as a 'site of constant reinvention',[52] and the 'reality of the internet means that we are dealing with the inherent and inexorable fluidity of evolving technologies.'[53] For these reasons it may be undesirable to introduce rigid technology-specific rules. As observed by Kirby J in *Dow Jones & Co Inc v Gutnick*,[54] such rules would have a limited lifespan and soon be rendered obsolete.[55]

However, some immediate change to the existing law is necessary. In particular, Australian courts should not be afraid of departing from a strict application of our existing defamation law, so as to better address the unique issues raised by social media. Legislative intervention is arguably required in some areas. For example, the introduction of a 'single publication rule' and a 'safe harbour' provision for internet intermediaries is long overdue. Social media will continue to change the way we communicate. It is clear that Australia's defamation law must change too.

Penelope Bristow is a law student at University of Queensland and was a finalist in the 2018 CAMLA Young Lawyers Essay Competition.

45 *Cassell & Co Ltd v Broome* [1972] AC 1027, 1071. See also *Crampton v Nugawela* (1996) 41 NSWLR 176, 195 (Mahoney ACJ); *Roberts v Prendergast* (2014) 1 Qd R 357, 357 [33] Gotterson JA).

46 *Mickle v Farley* [2013] NSWDC 295, [21] (Elkaim DCJ).

47 *Belbin v Lower Murray Urban and Rural Water Corporation* [2012] VSC 535, [217] (Kaye J).

48 [2016] WASCA 83.

49 See, eg, *Dabrowski v Greeuw* [2014] WADC 175, [27] (Neuberger LCJ).

50 See, eg, *Cairns v Modi* [2010] EWHC 2859, [29] – [30] (Tugendhat J).

51 See, eg, *Polias v Ryall* [2014] NSWSC 1692.

52 Lelia Green, *The Internet: An Introduction to New Media* (Berg, 2010) 1.

53 *Crookes v Newton* [2011] 3 SCR 269, [43] (Abella J).

54 (2002) 210 CLR 575.

55 *Dow Jones & Co Inc v Gutnick* (2002) 210 CLR 575, [125].

Profile: Bruce McWilliam

Commercial Director at Seven West Media and Seven Group Holdings

CAMLA Young Lawyers representative, Michael Boland, recently caught up with Bruce McWilliam to discuss his role as the Commercial Director of Seven, some of his career highlights to date, and his thoughts on the trajectory of the broader media industry.

MICHAEL BOLAND: On behalf of the CLB readers, thank you for taking the time to speak with us, Bruce. Your current role is the Commercial Director at Seven West Media and also at Seven Group Holdings, the holding company of the Stokes Group which has diversified interests including Caterpillar WA and NSW and Coates Hire, as well as holding 40% of the media company.

Can you give us some insight into what exactly your role entails?

BRUCE McWILLIAM: It is a very interesting role for a very active group that is always engaged in transactions of some kind or another. We have a lot of rights that need enforcing or clarifying so there is always plenty going on. I am lucky to have the support of an excellent legal and regulatory team and we carve the work up broadly in terms of everyone's specialties, although in a small team everyone is to some extent a generalist as well.

I'd like to think that we provide focused and commercially based advice to get to the most effective outcomes at the least cost, so that the various business units think of us as a resource rather than a hindrance. It can't be left unsaid that we do have a principal shareholder who has enormous insight and is very experienced and involved in the business, and we have the benefit of his thoughts and guidance on all aspects, together with two focused and successful chief executives and their teams.

BOLAND: Going back a little now, what initially drew you to the law? When you first set out in the profession, what were you hoping to achieve?

McWILLIAM: I always wanted to be a lawyer and was attracted to being a solicitor rather than a barrister, as I thought the bar would be more isolating. I do have quite a few friends who went to the bar and they all did very well and I often brief them. Some have gone to the bench and even the High Court. I always liked the interaction of the practical aspects of practice with the academic side of law, and used to lecture part time at Sydney University Law School in my early days which I found rewarding.

I started working part time at a law firm as soon as I could. Initially at Minter Simpson, which I greatly enjoyed, and then at Allens. I was always impressed by the excellence and dedication of the partners I worked for and the respect they commanded from their clients. The first guy I worked for remained a friend all my life and tragically recently died. But working for him was a wonderful Mad Men type of existence in the late 70s. He used to start work at 5 am and at 1 pm we'd take clients to lunch where a great time was had by all at the San Francisco Grill and other establishments. His secretary would have finished all his dictation and documents by the time he returned so he could polish them and distribute them to his clients. Allens was more sedate in some senses but the quality of both the work and the other lawyers was quite inspiring and I have many friends from there to this day. Quite a few Allens alumni also came to News Corp over the years and one is now the head of the ABC.

One thing I have been fortunate in, in my in-house roles, has been the quality of the external advice that I have had access to. I have always tried to deal with the best, rather than receive advice from faceless teams. If you have an expert helping you then the hourly rates give you a great outcome and you get the benefit of first class advice. The ability to deliver that quickly is a huge advantage.

BOLAND: How did your progression into media law and the media industries evolve? Was this always your plan?

McWILLIAM: I was always interested in media but actually got into it by chance. The partner at Allens I worked for was Kerry Packer's principal lawyer

so I started off doing Consolidated Press work at an early stage of my career. I always say that when I first met Kerry Packer I didn't know who he was except that I'd seen him interviewed on Parkinson! We were thrown in head first and as a result we learned a lot. I often wondered what the client thought of it! However I found it very stimulating and it was always sharp and quick work with no tolerance for slowness or indecisiveness which was a good discipline. The work was across many areas and all the people in the business were fascinating and good at what they did.

I quickly met Sam Chisholm who became a major source of work from Nine Network, and also from News Corp when he left to join Rupert Murdoch. Although I had known him at University, I also re-met Malcolm Turnbull, who joined Consolidated Press as General Counsel in 1982 from the bar, when that title and role seemed very American. Anyway Malcolm excelled at it and made his role a central one for the group. His interactions with Packer were unique. He also did a brilliant job in defending Packer against the Costigan Royal Commission, which was a misguided diviner of supposed criminal conduct and general wickedness and wasted vast sums of public money as well as needlessly ruining a lot of good people's lives. I gained enormous respect for how Malcolm calmly batted back every missive from the Royal Commission and took them on at their own game. At one point he issued a press release denouncing the methods of the Commission (which entailed a lot of leaking and little regard for confidential investigation). It was a hairy time but it turned out well and we learned a lot. Malcolm impressed me because he helped a lot of little people along the way who otherwise would probably not have been able to stand up to what they were unfairly accused of. It was McCarthyism at its worst. We must always bear in mind that the one-way exchanges demanded by Royal Commissions mean that nuanced answers count for little. You take legal protections for granted and as lawyers you have to be alive to when people try to circumvent or override them. That's what you mustn't forget about being a lawyer, that you can protect people. The rule of law is very important.

After Kerry Packer sold the TV stations to Alan Bond – facilitated by the change in the media laws – that also set us off on the trail of a lot of interesting work. In 1991 Chisholm asked me to go to London with him as he was made CEO of BSkyB, then a big loss-making operation and News Corp itself had only just come through a massive restructuring forced on it by the credit crunch and the demands of its huge banking syndicate. I enjoyed meeting with the English lawyers, such as at Allen and Overy and Herbert Smith. AO were brilliant banking lawyers who could use the considerable tools at their disposal to create simple structures which assisted the client wherever possible. Herbert Smith helped BSkyB play an early competition card which opened up a great commercial outcome. Later on, those awful EU strictures were turned against BSkyB - which the EU treated as a monopoly even though it was dwarfed by the huge European conglomerates. I always regarded the EU as a joint French and German attempt to screw the English!

The great thing about English lawyers is the confidence of the very good ones. I met some amazing barristers like Jonathan Sumption (now a leading judge) and George Carman who performed magnificently in summary judgment applications and were invaluable when you couldn't avoid litigation (and priced accordingly). They had shades of Rumpole of the Bailey, and their exploits were beloved of the tabloids. Incidentally I have always found our local solicitors and barristers to be just as good, even if less flashy.

When BSkyB successfully floated on the London and New York stock exchanges, News took over pay TV companies in Hong Kong, China and India, and then set about entering the European sphere, which brought Rupert Murdoch into contact with a lot of red tape and vested interests. That's what I've always admired about him, his ability to go into new fields and countries. Some of the media entrepreneurs of Europe were also fascinating people, very often pioneers, and always colourful. One became Prime Minister of Italy, another went spectacularly bankrupt when the banks unfairly foreclosed on him in 2002, but then he successfully turned the tables by winning a big action against the bankers.

BOLAND: Your career has placed you at the centre of very significant developments in the media both in Australia and overseas. What are some of the key learnings you've taken away from your experiences?

McWILLIAM: I have been very lucky in having worked for Packer, Murdoch and Kerry Stokes, and a lot of their top executives who were on top of their game. I always admired the mastery that the proprietors have over their businesses and the fields they operate in and the controlled risks they are prepared to take. You also meet a lot of

fascinating people in their counterparts they do business with. Their drive to succeed makes it very satisfying to be on their teams. Reporters and content producers are also dedicated and professional and it is our job to help them operate and succeed in their fields and achieve their best. In a small industry, you run across the same players time and time again so your enemy on one thing can be your valued ally on another, sometimes at the same time. Relationships are important and it's good to know when you can rely on people.

BOLAND: How would you describe the service you provide, and how would you describe the essential characteristics of a great lawyer?

McWILLIAM: You have to stay calm under pressure and not allow yourself to be compromised. Try to reduce things to simple elements. You have to know what your client wants to achieve and get them there with a minimum of fuss. At the end of the day media is an exciting field but it involves the same elements as any other legal problem in any other business. As I've said, I have been fortunate to work with some gifted professionals, lawyers and barristers. You need have to have a good network of specialists who can be counted upon to deliver at short notice.

BOLAND: Gazing into your crystal ball for a moment, how do you see the future of the Australian media landscape? What are some of the most urgent challenges?

McWILLIAM: People will always demand and flock to great content and information. The media landscape has always been full of challenges. Sam Chisholm said to me that Hollywood has always been successful at farming/exploiting the latest technology without loosening their grip on existing technologies and platforms. If you take newspapers, throughout history they have very often lost money, so they provide a service in many ways. I know proprietors don't try to incur losses, but the internet has created a lot of disruption, in media as well as a lot of other industries. Viewers aren't content to turn on a single channel now, they want to have seamless access to a lot of sources whenever they want. But there is still premium programming like news and sport, which, despite the plethora of ways of receiving it, is the most valuable live content and in that sense nothing changes, except perhaps the way you consume it. You have to be able to show viewers that you will meet their expectations and you have to show your advertisers that you will deliver it to wherever their customers are.

BOLAND: Are those challenges overwhelming, or are they simply opportunities for growth?

McWILLIAM: Hopefully opportunities for growth, although the cost pressures entailed in premium rights are enormous and squeeze margins. At the end of the day a media outlet has to provide their customers with what they want when they want it. And it has to facilitate the same access for its advertisers. The great tech platforms seem to exist outside the tax and regulatory hemisphere in many ways whilst harnessing huge cashflows, so it often doesn't seem like an even playing field – however, who listens when you complain!

BOLAND: What are your tips for young lawyers with a special interest in the media?

McWILLIAM: Go to a good firm and get as much experience as you can. It doesn't have to be a big firm, there are some amazing small players with niche practices. If you've got time to do a Masters in a specialised area - that is often a good entry point as it makes you someone your firm can put forward when an issue in your skillset arises. Remember you're a lawyer and you will only be of interest if you can bring those skills to the table. Avoid telling people what they want to hear, but by the same token try not to be too much of a handbrake. But there are so many angles for young lawyers to gain exposure whether it be privacy law, data, copyright, contracts, financing, corporate, securities, defamation, structuring, tax, etc. The internet brings its own challenges with take down issues and liability for third party posts. You can't drop your standards, so very often on, say, a rights or exclusivity point, you'll find a lot hangs on the correctness of your advice. Tools like iPhones make it easier to carry out your job no matter where you are, and everyone demands instant turnaround. Write articles for publications as that's a good way of pushing your profile and adding to legal knowledge. In our industry it really is an around the clock role as that's the level of service that's expected of you, but you won't get any prizes for being wrong.

Michael Boland is a Regulatory Affairs Executive at Seven Network

International Standards for Data Breach Notification?

In this second part of a two-part article, Peter Leonard looks at data breach notification regimes in comparative jurisdictions and considers the challenges which arise where a data breach occurs across multiple jurisdictions.

In many circumstances an APP entity conducting cross-border business may be required to notify affected individuals and regulatory authorities in Australia and one or more other jurisdictions, including European Union counties. Australian businesses need to be aware of the separate thresholds and time limits that will apply in different jurisdictions.

There is no international standard for data breach notification or the jurisdictional nexus or other locating factors that give rise to an obligation to notify in a particular jurisdiction. Often a data breach may need to be notified in multiple jurisdictions, in markedly different forms, even if the intrusion or other event that give rise to the obligation to notify occurred in only one jurisdiction. Sometimes the obligation will arise independently from the laws of the jurisdiction within which the intrusion or other event that give rise to the obligation to notify occurred.

Care should be taken in developing international data breach response plans to ensure that national variants are addressed.

United States of America

In the U.S.A., the US Congress has repeatedly attempted, but failed, to agree on federal data breach notification legislation. As a result, there is no single federal statute that imposes a breach notification obligation on most companies. 'Reasonable' security standards are still being debated. Nearly every U.S. state has a different breach notification law, with widely varying notification thresholds. 48 states and the District of Columbia have each passed their own laws that require notifications in certain circumstances. Alabama and South Dakota are the only states without breach notification laws.[1]

Many U.S. state data breach laws provide that a trigger for notification to the data protection authority is the likelihood or possibility of fraud or identity theft or other significant adverse consequence for affected individuals within the relevant state.

Canada

In Canada, the *Digital Privacy Act* of June 2015[2] amended Canada's federal private sector privacy law, the *Personal Information Protection and Electronic Documents Act* (**PIPEDA**). While other provisions of the Digital Privacy Act are now in force, those dealing with breach reporting, notification and recordkeeping will come into force after regulations outlining specific requirements are developed and in place.

On September 2, 2017, the Government of Canada published proposed 'Breach of Security Safeguards Regulations'.[3] The proposed regulations relate to the PIPEDA provisions not yet in force.

The PIPEDA provisions when in force will require an organisation to notify affected individuals, and report to the Office of the Privacy Commissioner of Canada (**OPC**), as soon as feasible, regarding any data breach which poses a "real risk of significant harm" to any individual whose personal information was involved in the breach. The breach provisions in PIPEDA specify that such notification and reporting must be done in accordance with regulations passed pursuant to PIPEDA.

Failure to notify the OPC of a security breach, as required by the PIPEDA provisions yet to come into force, is an offence, punishable by a fine of up to $100,000. PIPEDA also contains a private right of action for affected individuals, which could result in damages being awarded by the Federal Court of Canada for failure to notify affected individuals. This private right of action also opens the door to potential class actions for an organisation's failure to comply with the breach notification provisions in PIPEDA.

The proposed Breach Regulations specify that reports to the OPC must be in writing and must contain certain stipulated information, such as a description of the circumstances of the breach, the date or time period of the breach, an estimate of the number of affected individuals, a description of the steps taken to reduce the risk of harm, and a description of the organisation's notification or intended notification steps.

Notification to affected individuals must include similar information as provided to the OPC, and must also include:

- a toll-free number or email address that affected individuals can use to obtain further information about the breach; and

1 http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

2 Available through https://www.priv.gc.ca/resource/fs-fi/02_05_d_63_s4_e.asp

3 http://www.gazette.gc.ca/rp-pr/p1/2017/2017-09-02/html/reg1-eng.php

- information about the organisation's internal complaint process and about the affected individual's right to file a complaint with the OPC.

Acceptable methods of direct and indirect notification to individuals are also set out in the proposed Breach Regulations. Indirect notification may be given in circumstances such as where the giving of direct notification would cause further harm to the affected individual, where the organisation does not have the current contact information for affected individuals, or where the cost of giving direct notification is prohibitive for the organisation.

European Union

The new General Data Protection Regulation (**GDPR**) will introduce mandatory data breach notification across the European Union. The Article 29 Working Party[4] has recently completed a comment period on Guidelines on Personal data breach notification under Regulation 2016/679.[5] As at 12 February 2018 the Guidelines were adopted but not yet finalised.

Under Article 3 of the GDPR, a business (wherever resident and whether or not located in the EU or processing in the EU) controls or processes personal data of individuals in the EU if the processing is related to offering goods or services into the EU or monitoring the behaviour of individuals in the EU.

For the purposes of the GDPR, a data 'controller' determines the purposes and means of collection of personal data, and the 'processor' processes the information on their behalf.

"Processing" is not a concept of Australian privacy law. The term is broadly defined and essentially means any act or practice that is done to, or in connection with, personal information. In considering application of the GDPR, a business needs to review whether it:

- has an 'establishment' in the EU? (Article 3.1),
- offers good or services to individuals who are in the EU (whether or not for charge) (Article 3.2(a)), or
- monitors any behaviour of individuals in the EU (Article 3.2(b)).

Article 4 provides that the main establishment of a data controller is the "place of its central administration": that is, where "decisions on the purposes and means of the processing" occur. For processors, the main establishment will be either the place of central administration in the EU or, if the processor does not have one, then where the main processing activity in the EU takes place.

The GDPR recitals explain that a range of factors will be relevant to deciding whether a company is "offering goods or services" to individuals in the EU. These factors include:

- the use of language and currency or a top-level domain name of an EU Member State,
- delivery of physical goods to a Member State,
- making references to individuals in a Member State to promote the goods and services, and
- targeting advertising at individuals in a Member State.

Mere accessibility of an Australian company's website or app to individuals in the EU will not, by itself, reach the threshold.

Factors relevant to whether a processing activity is 'monitoring' the behaviour of individuals in the EU include whether a business is:

- associating individuals in the EU with online identifiers provided by their devices, applications, tools and protocols, such as IP addresses and cookie identifiers,
- tracking their behaviour on the Internet, and
- using data processing techniques that profile individuals, particularly in order to make decisions concerning them for analysing or predicting their personal preferences, behaviours and attitudes.

A "personal data breach" is notifiable[6] by a data controller to the relevant data protection authority "without undue delay and, where feasible, not later than 72 hours after having become aware of it". The WP29 expressed a view that a controller should be regarded as having become "aware" when that controller has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised. If notification is not made within 72 hours, the controller must provide a "reasoned justification" for the delay.

Whenever a breach affects the personal data of individuals in more than one Member State and notification is required, the controller will need to notify the lead supervisory authority, being the supervisory authority of the main establishment or of the single establishment of the controller. Therefore, when drafting its breach response plan, a controller must make an assessment as to which supervisory authority is the lead supervisory authority that it will need to notify.

The GDPR provides that when a data processor experiences a personal data breach, it must notify the data controller.[7] A data processor otherwise does not have relevant notification or reporting obligations under the GDPR.

4 http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

5 http://ec.europa.eu/newsroom/document.cfm?doc_id=47741

6 Notification to the authority must "at least": (1) describe the nature of the personal data breach, including the number and categories of data subjects and data records affected; (2) provide the data protection officer's contact information; (3) "describe the likely consequences of the personal data breach"; and (4) describe how the controller proposes to address the breach, including any mitigation efforts. If not all information is available at once, it may be provided in phases.

7 Article 33(2)

If a data controller determines that the personal data breach "is likely to result in a high risk to the rights and freedoms of individuals", the data controller must also communicate information regarding the personal data breach to affected data subjects. Under Article 32, this must be done "without undue delay". The GDPR provides exceptions to this additional requirement to notify affected data subjects in the following circumstances:

the controller has "implemented appropriate technical and organisational protection measures" that "render the data unintelligible to any person who is not authorized to access it, such as encryption";

the controller takes actions subsequent to the personal data breach to "ensure that the high risk for the rights and freedoms of data subjects" is unlikely to materialise; or

- when notification to each data subject would "involve disproportionate effort", in which case alternative communication measures may be used.[8]

A "personal data breach is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed". Note that unlike many data breach notification scheme, the requirements extend to destruction of data, or alteration of data, and not just disclosure of personal data information: as the Article 29 Working Party states it, to any of:

- a "confidentiality breach" - where there is an unauthorised or accidental disclosure of, or access to, personal data,
- an "availability breach" - where there is an accidental or unauthorised loss of access to, or destruction of, personal data, and
- an "integrity breach" - where there is an unauthorised or accidental alteration of personal data loss.[9]

However, Article 31(1) contains an exception to the general requirement for notification to the data protection authority of "personal data breach": notice is not required if "the personal data breach is unlikely to result in a risk for the rights and freedoms of individuals".

The relevant data protection authority may require notification, or conversely, determine (in effect, confirm) that it is unnecessary under the circumstances.

The GDPR includes large fines: up to 1,000,000 Euros or, in the case of an enterprise, up to two percent of its annual worldwide turnover.

Singapore

Section 24 of the Personal Data Protection Act obliges an organisation to protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

Under the Personal Data Protection Act as at February 2018, there is no explicit requirement for organisations to notify individuals in the event of a data breach. However, the Personal Data Protection Commission (**PDPC**) 'Guide to Managing Data Breaches' provides that it is good practice to notify individuals affected by a data breach.

The PDPC also considers the following as mitigating factors in the event of a breach:

- whether the organisation informed individuals of the steps they could take to mitigate risk caused by a data breach; and
- whether the organisation voluntarily disclosed the personal data breach to the PDPC as soon as it learned of the breach and cooperated with the PDPC's investigation.

However, Singapore is planning introduction of a mandatory data breach notification scheme.[10] In brief:

- The proposal by the PDPC is to mandate breach notification to both individuals and the PDPC under certain circumstances.
- In cases where there is a risk of impact or harm to the affected individuals, organisations should notify both the individuals and the PDPC.
- However, even when there is no risk of impact or harm to the affected individuals but where the scale of the breach is significant because it involves 500 or more individuals, then the PDPC only must be notified.
- The proposed timeframe for breach notification to the PDPC is 72 hours. For notification to individuals, no specific time frame is provided but they should be notified as soon as practicable.
- In the case of a data intermediary, there will be a requirement to immediately notify the organisation on whose behalf it is processing the personal data the event of a breach.
- These notification obligations will operate concurrently with other laws which apply to organisations such as financial institutions and critical infrastructure providers who have obligations to notify regulators under those laws. For example, on July 1 2014 the Monetary Authority of Singapore instructed financial institutions to report all security breaches within one hour of their discovery.

Peter Leonard is the Principal at Data Synergies and a Consultant at Gilbert + Tobin.

8 See Opinion 03/2014 on breach notification; also Guidelines on Personal data breach notification under Regulation 2016/679, pages 15 and 16

9 Opinion 03/2014 on breach notification; also Guidelines on Personal data breach notification under Regulation 2016/679, pages 6 and 7.

10 Public Consultation for Approaches to Managing Personal Data in the Digital Economy 27 July 2017 https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Legislation-and-Guidelines/publicconsultationapproachestomanagingpersonaldatainthedigitaleconomy270717f95e65c8844062038829ff000.pdf

Net Neutrality in Australia

Claudia Carr, a finalist in the 2018 CAMLA Essay Competition, provides some thoughts on the debate about the regulation of net neutrality in Australia, including the extra-territorial effect of the repeal of net neutrality regulations in the United States.

Introduction

On 14 December 2017, the United States Federal Communications Commission ('FCC') voted 3-2 in favour of repealing net neutrality regulations. The regulations, introduced under President Obama in 2015, sought to prevent internet service providers ('ISPs') from prioritising or privileging certain online content.[1] The vote to repeal those regulations proved divisive. FCC chairman Ajit Pai led the repeal, arguing that the regulations stifled telecommunications market growth.[2] That position met vociferous opposition from activists, Democrats, and large technology companies, such as Alphabet (the parent company of Google), Amazon, Facebook, Microsoft, Netflix and Dropbox, who argued that the repeal of net neutrality would bring about the end of the open internet.[3] Predictably, ISPs sided with Pai.[4]

Despite the fact that net neutrality is a hot button issue in America, it has been hardly discussed in Australia, and there is scant Australian legal scholarship on topic. This paper explains what net neutrality is and considers whether we have net neutrality in Australia. It goes on to discuss the extra-territorial effect in Australia of the American repeal of net neutrality regulations. Although it is unlikely that Australia will experience any immediately significant effects as a result of America's repeal, it is possible that in conjunction with other factors, the American repeal will spur a gradual decline in net neutrality in Australia. This paper explains why that is undesirable, and suggests that Australia consider adopting laws to safeguard net neutrality.

What is 'net neutrality'?

Net neutrality is the principle that ISPs should treat all online traffic and content equally and cannot give preference to certain digital content providers, or block consumers from particular sites, content, or services.[5] According to this principle, consumers do not have to pay more to access certain online content or to access faster internet speeds. Digital content providers do not have to pay fees for their online content to be prioritised for consumer viewing.

Net neutrality recognises that the internet is a vital resource in the twenty-first century, and so ought to be accessible to all equally. The American net neutrality regulations prohibited ISPs from blocking legal content, applications, services or non-harmful devices, impairing or degrading lawful internet traffic on the basis of legal content, applications, services, or non-harmful devices, or favouring particular lawful internet traffic over other lawful traffic for consideration. They also prevented ISPs from unreasonably interfering with or disadvantaging consumers' ability to select, access, and use lawful online content, applications, services, or devices.

The rationale for net neutrality is persuasive. The internet is a major source of information for the public.[6] When advocating for net neutrality and the characterisation of the internet as an essential utility, President Obama said 'there are no toll roads on the information superhighway'.[7] Proponents of net neutrality argue that America's repeal will hurt consumers: net neutrality preserves healthy competition in the telecommunications market.[8] Google said that 'the Internet should be competitive and open… no Internet access provider should block or degrade Internet traffic, nor should they sell "fast lanes" that prioritize particular Internet services over others'.[9] Without net neutrality, ISPs may discriminate between consumers.[10] Consumers might have to choose their internet service providers based on what content those companies provide access to – in the process, sacrificing access to other content. This may also stunt innovation in the development of online content.[11]

1 *Protecting and Promoting the Open Internet*, 80 FR 19737, 19737–19850.

2 Ajit Pai, *How the FCC can Save the Open Internet* (21 November 2017) The Wall Street Journal <https://www.wsj.com/articles/how-the-fcc-can-save-the-open-internet-1511281099>.

3 Kara Alaimo, *How Google and Facebook could Save Net Neutrality* (7 December 2017) Bloomberg <https://www.bloomberg.com/view/articles/2017-12-06/how-google-and-facebook-could-save-net-neutrality>.

4 Andrew Nusca, *Net Neutrality Explained: What it Means (and Why it Matters)* (23 November 2017) Fortune <http://fortune.com/2017/11/23/net-neutrality-explained-what-it-means-and-why-it-matters/>.

5 However, the definition of net neutrality different according to different sources. See further James Endres, 'Net Neutrality – How Relevant is it to Australia?' (2009) 59(2) *Telecommunications Journal of Australia* 22.1, 22.3.

6 Matt Liddy, *Australians don't trust the news* (16 January 2015) ABC <http://www.abc.net.au/news/2015-06-16/australians-digital-news-trust/6548232>.

7 Peter Suciu, *Obama and net neutrality: What it means* (10 November 2014) Fortune <http://fortune.com/2014/11/10/obama-net-neutrality-explained/>.

8 Endres, above n 5, 22.2.

9 Nusca, above n 4.

10 Endres, above n 5, 22.2.

11 Richard French, 'Net Neutrality 101' (2007) 4 *University of Ottawa Law and Technology Journal* 109, 125.

Opponents of net neutrality argue that the internet does not need to be regulated. The justification for this argument posits that net neutrality regulations hurt investment; 'red-tape' should be reduced to encourage market growth and healthy competition.[12] Part of the issue is that ISPs are facing increased traffic through their networks, which requires them to incur costs to conduct network upgrades. Meanwhile, online content providers that are driving the increase in online traffic (such as Netflix and Stan) are profiting from the increased distribution of their content. Arguably, internet service providers should be permitted to recover their costs through non-neutral models, such as by charging consumers more to access certain content. Non-neutral models also allow ISPs to ensure that internet service is not degraded by managing different kinds of online traffic in different ways.[13]

Do we have net neutrality in Australia?

Before we can consider the extra-territorial effect of America's repeal of net neutrality regulations, we need to determine whether net neutrality currently reigns in Australia. At present, there are no Australian laws that regulate or enforce net neutrality. However, for the most part, Australians enjoy equal access to the internet.[14]

Despite the lack of regulation, several factors contribute to the prevalence of net neutrality in Australia. First, Australian consumers pay for a certain amount of internet usage per billing period, unlike in the US.[15] Thus, Australian ISPs are less affected by prolific growth in online traffic; their customers' data usage is capped and those who use more pay higher fees. Second, the ISP market in Australia is much more competitive than that in America, with low barriers to entry.[16] If one ISP were to break tradition and implement non-neutral practices, consumers could switch providers. Third, the Australian Consumer Law prohibits misleading and deceptive conduct in trade or commerce, which would require ISPs to disclose any practices that restricted consumer use of the internet.[17] For example, when Telstra sought to slow the delivery of certain content for particular customers, ACCC Chairman Rod Sims stated that where ISPs treat particular online traffic differently, those providers must be transparent and ensure that 'customers can easily understand the implications of these practices on the services they receive'.[18]

Fourth, Australia's competition laws prohibit ISPs from abusing their market power in a way that substantially lessens competition.[19] Section 151AJ of the *Competition and Consumer Act 2010* (Cth) pertains specifically to the telecommunications market. It provides that an ISP that has a substantial degree of market power engages in anti-competitive conduct if it takes advantage of that power in the telecommunications or any other market with the effect or likely effect of substantially lessening competition, or takes advantage of that power combined with other conduct with the combined effect or likely effect of substantially lessening competition. Section 151AJ(6) provides that an ISP may engage in anti-competitive conduct even if its conduct involves the exercise of an existing legal or equitable right. Despite the fact that the law does not prohibit non-neutral practices, those same practices are still capable of contravening competition law. Thus, it would be risky for a dominant market player to adopt non-neutral practices.

Finally, protection of net neutrality can also be found in Pt XIC of the *Competition and Consumer Act 2010* (Cth). That part sets out the telecommunications access regime, which is the process by which ISPs may obtain access to input services. ISPs do not have a general right of access – the ACCC must 'declare the service', before which it conducts a public inquiry to determine whether that access will promote the long-term interests of users of the service.[20] Subsequently, the provider can be requested to supply services on non-discriminatory terms. The provider must also comply with the standard access obligations, which require particular standards of services.[21] Endres argues that Pt XIC 'negates the need for a specific net neutrality rule'.[22]

Despite the above factors, non-neutral practices are present in Australia. O'Halloran claims that the subtlety of those practices allows them to 'continue unabated', rather than making them less harmful than more overt contraventions of net neutrality principles.[23]

12 Pai, above n 2.

13 French, above n 11, 124.

14 See also Cheng Lim and Ian Ranson, 'Net neutrality: the Federal Communications Commission's new Open Internet Order' (2015) 2(4) *Australian Media, Technology and Communications Law Bulletin* 39.

15 Endres, above n 5, 22.6.

16 Ibid 22.5; Bryon Frost, 'Net Neutrality – Overseas Experiences and Australia' (2015) 34(2) *Communications Law Bulletin* 5.

17 *Competition and Consumer Act 2010* (Cth) sch 2; Endres, above n 5, 22.7.

18 Frost, above n 16, 12.

19 *Competition and Consumer Act 2010* (Cth) s 151AJ.

20 Ibid s 152BCA.

21 Ibid s 152AR.

22 Endres, above n 5, 22.8.

23 Xavier O'Halloran, 'Net neutrality: "if you can't control the arteries…get hold of the blood"' (2015) 23 *Australian Journal of Competition and Consumer Law* 129, 129.

Within Australia, several ISPs carry on the practice of 'zero rating', which does not align with the principle of net neutrality.[24] Zero rating occurs when ISPs do not count particular internet usage towards a consumer's total usage allowance.[25] For example, at the time of writing, Telstra offers consumers a deal in which usage of the Australian Football League ('AFL') application and website to watch football games does not count towards the consumer's usage allowance – ie, the consumer can watch as much football as he or she would like without contributing to or exceeding his or her data allowance. Non-Telstra customers can still access mobile broadcasts of AFL, but it will count towards their usage allowance. Although zero rating is permitted in Australia, several other countries prohibit the practice.[26] While it advantages consumers in the short-term, O'Halloran expresses concern that, in the long term, consumers will end up paying for zero rating in the form of decreases in competition and choice.[27] When Netflix launched in Australia, it initially engaged in zero rating, but later abandoned the practice for being contrary to the company's support for net neutrality.[28]

Although Australians benefit from a mostly neutral net, there is nothing stopping ISPs from adopting other non-neutral practices in future. While Australian ISPs do impose data caps on consumers, growth in the use of streaming services may degrade the quality of internet services and necessitate service upgrades. The cost of those upgrades may yet see ISPs adopt non-neutral practices in Australia.[29] Further, there has been a recent increase in the development of network virtualisation technologies.[30] Network virtualisation involves the simulation of hardware, such as an internet server, in virtual software. North and Pascoe posit that there will 'almost certainly be net neutrality implications' as a result; networks may be managed so that they behave differently for different services, making it difficult to maintain neutrality.[31]

The introduction of the National Broadband Network ('NBN') may also signal the decline of net neutrality in Australia. NBN Co offers four different kinds of traffic classes, which allows ISPs to offer different classes of services to different classes of consumers.[32] Frost identifies this as a 'form of paid prioritisation which demonstrates that one of the key rules has already been thwarted in Australia by commercial [realities] of a future need for slow and fast lanes'.[33] However, Frost believes that market forces will self-regulate such that there is no need to be concerned about the effect of the NBN on net neutrality.[34] While this may be true with respect to consumers' ability to access online content, it does mean that certain consumers benefit from faster internet speeds.

It remains to be seen whether Australian lawmakers will weigh in on whether net neutrality should be regulated in Australia. In the past, net neutrality principles have been treated as important by lawmakers. In 2008, the Rudd government's proposed reforms to the *Broadcasting Services Act 1992* (Cth) were dumped pursuant to criticisms, including the concern that the reforms contradicted net neutrality principles.[35] The reforms involved requiring ISPs to block certain online content in an effort to make the internet safer for children. The introduction of net neutrality laws in other countries exemplify a path by which Australia may maintain equality of internet access for consumers.[36] However, Frost contends that net neutrality will never find strong support in Australia, and that the strength of the ACCC will negate the need for net neutrality rules.[37]

The effect of the American vote on net neutrality in Australia

America's repeal of its net neutrality regulations is unlikely to have any immediately significant impact on Australian consumers, ISPs, or online content providers. For the reasons identified above, Australia is not likely to see the sudden, overt introduction of non-neutral practices. The ACCC says that America's repeal will not affect Australians,[38] suggesting that

24 Ibid.

25 Lim and Ranson, above n 14.

26 See, eg, *Telecommunications Act* (Netherlands) art 7.4a; *Network Neutrality: Guidelines for a Neutral Internet* (24 February 2009) (Norway); European Union Regulatory Framework for Electronic Communications, Directive 2002/21/EC on a common regulatory framework for electronic communications networks and service, OJL 108, 24.4.2002.

27 O'Halloran, above n 23, 130.

28 James Elton-Pym, *Australia's competition regulator says existing laws should be enough to stop internet providers teaming up with content makers like Netflix to create content monopolies* (21 December 2017) SBS <https://www.sbs.com.au/news/will-the-us-net-neutrality-decision-affect-australian-internet-users>.

29 Cheng Lim and Ian Ranson, 'Net neutrality and Netflix' (2015) 2(5) *Australian Media, Technology and Communications Law Bulletin* 64.

30 James North and Richard Pascoe, 'Network virtualisation — what will it mean for communications regulation?' (2016) 3(3) *Australian Media, Technology and Communications Law Bulletin* 26.

31 Ibid 29.

32 Frost, above n 16, 14.

33 Ibid.

34 Ibid.

35 Alana Maurushat, David Vaile and Alice Chow, 'The aftermath of mandatory internet filtering and s 313 of the *Telecommunications Act 1997* (Cth)' (2014) 19 *Media and Arts Law Review* 263, 265; David Vaile and Renee Watt, 'Inspecting the Despicable, Assessing the Unacceptable: Prohibited Packets and the Great Firewall of Canberra' [2009] *University of New South Wales Faculty of Law Research Series* 35.

36 O'Halloran, above n 23, 131.

37 Bryon Frost, above n 16, 11–2.

38 Elton-Pym, above n 28.

Australia's existing laws are likely to be sufficient to deal with any issues that may arise.[39]

However, it is arguable that America's repeal, in conjunction with zero rating and changing technologies, could result in Australia seeing an insidious long-term decline in net neutrality. One internet advocate suggests that the American regulations acted as a standard according to which Australian internet service providers operated; without those regulations, Australian providers may seek to move away from more neutral practices in accordance with precedent behaviour emerging from America.[40] So long as their behaviour does not contravene Australian competition or consumer laws, ISPs are free to engage in non-neutral practices as they wish.

The repeal may result in higher costs for certain online services. If online content providers, such as Netflix, are forced to pay fees to American ISPs for the prioritisation of their content, those costs may be passed onto consumers globally.[41] The repeal may also affect Australians who engage in online business catering to American consumers. If they rely on American servers to reach overseas consumers, those businesses may see an increase in costs, or even the failure of some smaller servers.[42]

The long-term effect of America's repeal will depend on whether Australia legislates to protect net neutrality. While America's new position may encourage non-neutral conduct in Australia, it's worth noting that not all non-neutral practices are per se harmful.[43] For example, the different traffic classes adopted by NBN Co is an arguably harmless practice: it simply allows ISPs to cater for consumers with different needs. The needs of a large-scale corporation are different to that of individual user at home. Any potential laws on net neutrality may differentiate between different kinds of non-neutral conduct for that reason.

While currently allowing small concessions, Australia should remain vigilant about adhering to the broader principles of net neutrality. The erosion of net neutrality risks the health of the telecommunications market and may disadvantage consumers. Most importantly, the erosion of net neutrality will allow ISPs to control the content that customers can access online. The health of Australian democracy depends on access to information, and information is increasingly garnered via online sources.[44] A serious risk would present in allowing ISPs to prioritise particular online content, such as news sources. Those providers would have the opportunity to serve the political agenda of their parent company by prioritising favourable news sources. The wealthiest content providers could pay ISPs to prioritise their content for customers.

These risks are far removed from current practices like zero rating, and it is highly unlikely that they will manifest in Australia as a result of recent developments in America. However, a gradual decline in net neutrality is something to be wary of. For that reason, the introduction of net neutrality laws in Australia should at least be considered.

Conclusion

Australia currently enjoys relative net neutrality. Although America's repeal of its net neutrality regulations is unlikely to have any short-term impact in Australia, in the long-term, it may increase the relevance of the net neutrality debate in Australia by encouraging non-neutral conduct. The risks presented by that possibility make it worthwhile to at least consider the adoption of net neutrality laws in Australia.

Claudia Carr is a student at Curtin Law School and was a finalist in the 2018 CAMLA young lawyers essay competition with a version of this essay.

39 Ibid.

40 Flint Duxfield, *Net neutrality: US ruling could affect internet access in Australia, groups warn* (16 December 2017) ABC <http://www.abc.net.au/news/2017-12-16/net-neutrality-us-decision-could-affect-australians/9265056>.

41 Tara Donnelly, *What is net neutrality (and how does it affect Australians)?* (15 December 2017) WhistleOut <https://www.whistleout.com.au/Broadband/News/what-is-net-neutrality-and-how-does-it-affect-australians>.

42 Ibid.

43 Endres, above n 5, 22.4.

44 Vaile and Watt describe the degradation of net neutrality as 'Orwellian': David Vaile and Renee Watt, 'Inspecting the Despicable, Assessing the Unacceptable: Prohibited Packets and the Great Firewall of Canberra' [2009] *University of New South Wales Faculty of Law Research Series* 35.

Heavy Secrets: The Filing Cabinet Papers

"Those journalists who have been prepared to fight for the principle that stories that advance the public interest should be published have usually been vindicated. At every stage, the media must insist upon their right to investigate and to publish such stories: if they are right in their identification of the public interest, they are unlikely to come to harm in the long run."[1]

In February 2018, Australians were captivated by the story of the cabinet files cabinet papers. In Canberra in mid-2017, at a second-hand auction house selling used government supplies, a man purchased two filing cabinets for $10 each. According to media reports, the filing cabinets were sold at the bargain price of $10 on the basis that they were heavy, and the auction house selling them did not have keys for them.

After taking the heavy filing cabinets home and drilling holes in the locks, the man discovered that the filing cabinets contained cabinet papers from the Howard, Rudd, Gillard and Abbott governments. He contacted Michael McKinnon at the Australian Broadcasting Corporation (**ABC**), and according to reports published by the ABC McKinnon told the man that he should seek his own legal advice before handing over the cabinet papers. After a few weeks, the man called McKinnon back and over a number of months the cabinet papers were handed over to the ABC. Instead of "doing a Wikileaks", and publishing all of the cabinet papers online, ABC journalists went through the cabinet papers, authenticated each document and established whether there were stories of public interest that could be published by the national broadcaster that would not also be a national security threat. The identity of the purchaser of the filing cabinets who contacted McKinnon, was not revealed by the ABC.

In an article published by the ABC, ABC journalist John Lyons stated that he had: 'been appalled when WikiLeaks in 2016 did one of their "dumps" of thousands of documents which revealed information which in my view had no public interest… WikiLeaks had published medical files belonging to scores of ordinary citizens while many hundreds had had sensitive family, financial or identity records posted to the web.'[2]

The ABC was resolute, and according to media reports, not only did journalists contact those in the documents for comment, they only published information and documents on the basis of public interest. In response, the Australian Security Intelligence Organisation (**ASIO**) sent safes with combination locks to the ABC's offices. After negotiations between the ABC and the Commonwealth Government, the ABC reported that its main concern was the protection of its source (the man who had originally contacted McKinnon and handed over the documents), and the cabinet papers were returned to the Commonwealth Government. Critics characterised this as a failure to publish. The filing cabinet papers story illustrates the delicate balance between the public interest and national security in Australian law.

Australia has no constitutional equivalent to the First Amendment express guarantee set out in the US Constitution to hang public interest publications on. There is however the Constitutional implied freedom of political communication on government and political matters. As Michael Chesterman argues: 'freedom to communicate on matters of public interest is an integral element of any genuinely democratic society.'[3] Certainly freedom of expression aids self-government and democracy through the generation of open discussion on matters of public interest.[4] This entails recognition that freedom of the press is fundamentally in the public interest, and integral to the free flow of information, a functioning democracy and society, the administration of justice and open justice, informed political decision making and accountability.[5] Traditionally a number of subjects have been considered matters of general public interest, including: the conduct of those seeking political office or public trust;[6] politics and affairs of the national and local government;[7] government policy;[8]conduct of trade unions;[9]

1 Geoffrey Robertson and Andrew Nicol, *Robertson & Nicol on Media Law* (4th edition, Sweet & Maxwell: London, 2002), xv.

2 John Lyons, 'The Cabient Files: How classified documents were found at a Canberra second-hand shop', 3 February 2018, http://www.abc.net.au/news/about/backstory/news-coverage/2018-02-03/the-cabinet-files-and-how-they-were-found/9393008.

3 Michael Chesterman, *Freedom of Speech in Australian Law: a delicate plant* (Ashgate: Dartmouth, 2000), 301.

4 Andrew Kenyon, 'What Conversation? Free Speech and Defamation Law' (2010) 73(5) *The Modern Law Review* 697.

5 British Royal Commission on the Press, Final Report. (Cmd. 6810, 1977), 8–9, cited in Geoffrey Robertson QC and Andrew Nicol QC, *Robertson & Nicol on Media Law* (5th Edition, Law Book Company: 2007), vii.

6 *Slatyer v Daily Telegraph Newspaper Co* (1907) 7 SR(NSW) 488; *Whitford v Clarke* [1939] SASR 434; *Roberts v Bass* [2002] 212 CLR 1.

7 *Slim v Daily Telegraph* [1968] 2 QB 157 (CA); *Stephens v West Australian Newspapers Ltd* (1994) CLR 211

administration of justice and fair and accurate reporting;[10] public institutions, local authorities and administration of these institutions and authorities;[11] religious affairs; waste and extravagance on a public project;[12] police corruption;[13] and recently, political donations and obtaining access to a politician.[14] All these matters of public interest have the flavour of governmental and political matters.

This implied right is coupled with the fact that journalistic reporting in Australia is not restricted on the basis of media specific registrations, licences, accreditations or other permissions required for entities or individuals to engage in newsgathering activities. Despite the regulation of broadcasting more generally, there are also no media specific registrations, licences, accreditations or other permission required in Australian entities or individuals to sell news content to local news and media outlets. In contrast, the content produced by journalists and media organisations in Australia is highly regulated. All media organisations broadcasting or publishing content in print or online in Australia must comply with Australian intellectual property, contempt, defamation, varying State and Territory statutory reporting restrictions, and privacy laws (noting that there are exemptions for media organisations under the *Privacy Act 1988* (Cth) in circumstances where journalists commit to observing published written standards that deal with privacy).

More specifically when it comes to the issue of national security, section 79 of the *Crimes Act 1914* (Cth) (**Crimes Act**) and the *Criminal Code 1995 Act* (Cth) schedule 1 (**Criminal Code**) prohibit the disclosure of official secrets, which would prejudice national security or defence. Specifically, the disclosure of official secrets to unauthorised persons with the intention of prejudicing the Commonwealth's security or defence, or giving an advantage to another country. It can also be an offence to receive this type of information, if the recipient (in this case a journalist) knew or had reasonable grounds to believe that the material was communicated in contravention of the Crimes Act or the Criminal Code. Section 80.3 of the Criminal Code provides for defences for acts done in good faith, including where a person publishes in good faith a report or commentary about a matter of public interest.

Section 92 of the *Australian Security Intelligence Organisation Act 1979* (Cth) (**ASIO Act**) and section 41 of the *Intelligence Services Act 2001* (Cth) (**Intelligence Services Act**), also include provisions that prevent publication of material that might identify a person as an ASIO or Australian Secret Intelligence Service (**ASIS**) officer, employee or agent. Further to this, section 35P of the ASIO Act prohibits the unauthorised disclosure of information relating to covert operations designated "special intelligence operations" (which could include Australian Federal Police operations that relate to "special intelligence operations"). A contravention of this provision carries a penalty of 5 years imprisonment, or 10 years where the disclosure endangers the health or safety of any person or prejudices the effective conduct of a "special intelligence operation." Section 15K provides for a similar offence in relation to a "controlled operation". There is no journalist immunity or public interest defence to the offences, however recklessness is the requisite degree of fault.

On 7 December 2017, the Commonwealth Government introduced the *National Security Legislation (Espionage and Foreign Interference) Bill 2017* (Cth) (**National Security Bill**) to strengthen existing espionage, secrecy, treason, sabotage and related offences, introduce new offences targeting foreign interference and economic espionage, and establish a Foreign Influence Transparency Scheme. The National Security Bill amends the Crimes Act, Criminal Code and *Telecommunications (Interception and Access) Act 1979* and makes consequential amendments to other legislation to reform the Commonwealth's secrecy offences, including the criminalisation of leaks of harmful information and the possession of sensitive information that is in the national interest.

Of most relevance to journalists, is subsection 122.5(6) which will provide a defence to prosecution for an offence relating to the dealing with or holding of information, if the person dealt with or held the information in the public interest and in the person's capacity as a journalist engaged in fair and accurate reporting. As set out in the Explanatory Memorandum, this extension of the defence to a person who deals with or holds information would allow journalists to undertake a range of activities, such as collecting and holding information received from a source in the course of researching, writing or editing a story and determining an appropriate balance between competing public interests and filtering out stories that are not in the public interest. In the draft

8 *ACP v Uren* (1966) 117 CLR 185.

9 *Duane v Granrott* [1982] VR 767.

10 *Chakravarti v Advertiser Newspapers Ltd* (1998) 193 CLR 159; *Rogers v Nationwide News Pty Ltd* [2003] HCA 51.

11 *Renouf v Federal Capital Press of Australia Pty Ltd* (1977) 17 ACTR 35; *Bellino v Australian Broadcasting Corporation* (1996) 185 CLR 183

12 *Johnston v Australian Broadcasting Corporation* (1993) 113 FLR 307.

13 Hardie v The Herald and Weekly Times Pty Ltd [2015] VSC 364.

14 *Hockey v Fairfax Media Publications Pty Limited* [2015] FCA 652.

legislation, the term 'journalist' is not limited in any sense to those acting in a professional capacity, and is given its ordinary and natural meaning. The Explanatory Memorandum refers to the Macquarie Dictionary definition of 'journalist' as a person engaged in 'journalism', being 'the business or occupation or writing, editing, and producing photographic images for print media and the production of news and news analysis for broadcast media.' And the Oxford Dictionary definition of 'journalist' as 'a person who writes for newspapers, or news websites or prepares news to be broadcast'. However, the defence will only apply to a journalist 'engaged in fair and accurate reporting'. This is similar to the fair and accurate reporting concept used within section 18D of the *Racial Discrimination Act 1975* (Cth). The requirement for journalists to be engaged in fair and accurate reporting will therefore limit the scope of the defence, and will exclude those who are publishing information or documents without engaging in fair and accurate reporting, who are using information or documents to produce false or distorted reporting, or those who are not journalists engaged in fair and accurate reporting. In addition, the defence will only be available where the conduct is in the public interest (in accordance with section 13.3 of the Criminal Code). However, dealing with or holding certain information will not be in the public interest. This includes information protected by section 92 of the ASIO Act and section 41 of the Intelligence Services Act (protecting the identity of ASIO and ASIS officers, employee or agents respectively), individuals protected under the *Witness Protection Act 1994* (Cth), or where it is information that will or is likely to harm or prejudice the health or safety of the public or a section of the public. The defendant bears the burden of proof, and the Explanatory Memorandum stresses that a journalist should be able to point to evidence that their conduct was done in the public interest and in their capacity as a journalist engaged in fair and accurate reporting. Further to this, section 123.1 of the Bill proposes that injunctions may be used to restrain a person from contravening a provision of Division 122 of the Bill.

Media organisations, journalists and lawyers have been critical of the National Security Bill. In response to the National Security Bill. The Media Entertainment Arts Alliance (**MEAA**) recommended that to protect public interest reporting, a general public interest and news reporting defence be included for all relevant provisions in both the secrecy and espionage sections of the National Security Bill. The Law Council provided a submission to the Parliamentary Joint Committee on Intelligence and Security's Inquiry into the National Security Bill. This submission stressed the Law Council's concern that many of the offence provisions are broadly drafted to capture a range of benign conduct that may not necessarily amount to harm or prejudice to Australia's interests. Of particular concern to the Law Council is the broad definitions of key terms, and the potentially broad application of these measures. The Law Council proposed that a narrowing of the provisions would provide both greater clarity regarding their operation and the protection of national security, while also addressing concerns that some of the provisions are not a necessary or proportionate limitation on freedom of expression and the Constitutional implied freedom of political communication.

The National Security Bill was referred to the Parliamentary Joint Committee on Intelligence and Security in December 2017, and was considered by the Senate Standing Committee for the Scrutiny of Bills and the Parliamentary Joint Committee on Human Rights in February 2018.

Australian law in respect of the publication of Government secrets will continue to be a source of tension between those concerned with public interest journalism and investigative reporting freedom of the press and freedom of speech, on the one hand, and national security on the other.

Katherine Giles is a Senior Associate at MinterEllison specialising in intellectual property, entertainment and media law, and prior to August 2016 was a Senior Lawyer at the ABC.

6 Things You Should Know About the New NDB Scheme

Valeska Bloch, a partner at Allens, takes us through some of the key issues arising out of the new notifiable data breach scheme.[1]

The Office of the Australian Information Commissioner (***OAIC***) recently reported that sixty-three data breaches were notified to it in the first six weeks of the new notifiable data breaches scheme (**NDB scheme**) taking effect. Although the basic components of the scheme are now reasonably well known, organisations are still grappling with the practicalities of assessing and notifying data breaches, particularly in circumstances where the facts are unclear and the data the subject of the breach was jointly held. This article attempts to provide some practical guidance in navigating the new scheme.

1 The 30 day time limit to assess whether an eligible data breach has occurred is not a hard stop.

Where an entity becomes aware of reasonable grounds to suspect that an *eligible data breach* has occurred, it must carry out an assessment of this suspicion expeditiously and must take *all reasonable steps* to carry out this assessment within 30 days.[2]

The OAIC has said that entities should treat this 30 day period as the maximum time limit, particularly given that the risk of serious harm to individuals tends to increase with time. However, the OAIC also recognises that it will not always be possible to complete an assessment of a suspected data breach within 30 days, for example, if systems or records were lost during the intrusion and significant recovery effort is required.

Top tip: Where an entity cannot reasonably conduct a data breach assessment within 30 days, the OAIC recommends that an entity prepare and retain documentation that will allow it to demonstrate:

- that all reasonable steps were taken to complete the assessment within 30 days;
- the reasons for the delay; and
- that the assessment was reasonable and expeditious.

2 The scheme does not apply to employee records.

The OAIC has confirmed in its *Data breach preparation and response* guide that businesses will not be required to notify the OAIC or individuals about data breaches relating to employee records – that is, personal information of an employee relating to their employment. This is because the employee records exemption provided for in the *Privacy Act 1988* (Cth) (*the **Privacy Act***) applies to the NDB Scheme.[3]

A few words of caution.

- Even where the employee records exemption applies, the OAIC recommends notifying individuals affected by a breach of employee record if it is likely to result in serious harm.
- Think carefully about whether the information involved in a data breach is *truly* covered by the exemption.

For example, employees often use their work email accounts to receive personal emails, such as communications from their bank which would not be covered by the exemption. In practice, it may be difficult to distinguish between what data does and does not fall within the exemption.

- The employee records exemption will not extend to a data breach involving tax file numbers.[4]
- The employee records exemption only applies to an employee record held by the employer. If your organisation stores its employee records with a third party, the exemption will extend to a data breach involving those records and your service provider will need to notify the OAIC of the breach.

3 The OAIC can make a declaration that an entity does not have to notify, or can defer notification, for a specified period.

The NDB Scheme allows the OAIC to declare that an entity may dispense with or delay notification following an *eligible data breach*.[5] The decision to exercise this power may be on the OAIC's own initiative or follow an application by an entity that has experienced a data breach.[6]

In deciding whether to make such a declaration, the Commissioner must be satisfied that it is reasonable in the circumstances to do so, having regard to:

1 Thank you to Sam Dutaillis and Alexi Polden for their assistance in preparing this article.
2 *Privacy Act 1988* (Cth), s 26WH.
3 *Privacy Act 1988* (Cth), s 7B.
4 *Privacy Act 1988* (Cth), ss 17, 18 and 26WE(1)(d).
5 *Privacy Act 1988* (Cth), s 26WQ.
6 *Privacy Act 1988* (Cth), s 26WQ(5).

1. The public interest;
2. Any relevant advice provided to the OAIC by an enforcement body or the Australian Signals Directorate; and
3. Any other matter that the OAIC considers to be relevant to the situation.[7]

The OAIC has also identified a number of additional factors that they may consider before making a declaration to this effect, including whether the risks associated with notification outweigh the benefits to individuals at risk of serious harm.

Things to consider when making an application:

- The OAIC expects that declarations will only be made in exceptional circumstances. Unfortunately, owing to the practical reality that only entities which are granted declarations will be made aware of the circumstances in which they occur, it is difficult to predict what will be considered sufficiently *'exceptional'*.
- Entities that request an exemption should be prepared to present a compelling case with detailed evidence as to why it is reasonable in the circumstances for the notification requirements to be dispensed with, including why no other exemptions apply.

4 You may still need to notify even if the eligible data breach requirement is not triggered

It is a common misconception that once a data breach has occurred, your notification obligations are limited to those required by the NDB scheme. In fact, there may be other good reasons why you may choose or need to notify.

1. APP 11 – Prior to the introduction of the NDB scheme, the OAIC had suggested that in certain circumstances, a failure to notify may in and of itself constitute a breach of APP 11. This is because notifying may in fact enable individuals to protect their personal information, for example, by changing their passwords.

Although the introduction of the NDB Scheme makes it less likely that the OAIC would seek to assert that a breach of APP 11 has occurred in a data breach scenario, it is still open to the OAIC to do so. This means that even if you suffer a data breach that is not an eligible data breach, you should still consider notifying.

2. Continuous disclosure – If you are a listed entity and there is a possibility that a data breach you suffer might reasonably be expected to have a material effect on the price of your securities, you may need to disclose the data breach to the ASX.

3. Other notification requirements – Depending on the nature of your business, how and where you hold your data and who you hold data about, you may be subject to other notification requirements, for example, under state-based or international data protection laws, or under sector specific laws. Keep in mind:

The EU General Data Protection Regulation (***GDPR***) which has significant extra-territorial reach.

Reporting obligations under the National Cancer Screening Register Act 2016 and the My Health Records Act 2012.

4. Public and customer relations – Even if there is no legal obligation to notify affected customers, you may decide to notify about a non-eligible data breach in the interests of maintaining good public relations, particularly if there is a reasonable chance that the data breach may become public through sources that are out of your control. If you get on the front foot with notification and a public statement, you can control the narrative and ensure that your customers receive accurate information.

5 You will be liable for the notification of breaches suffered by an overseas recipient of personal information

Ordinarily, where an entity discloses personal information to an overseas recipient in accordance with Australian Privacy Principle 8.1, the disclosing party will only be liable for a breach of the Australian Privacy Principles (***APPs***) by that overseas recipient where the APPs ***do not*** apply to the overseas recipient.[8]

The NDB scheme takes a stricter approach, such that a party who discloses personal information in accordance with APP 8.1 is deemed liable even where the overseas recipient is itself subject to the Privacy Act.[9] Keep in mind that this deemed liability will not apply to personal information disclosed overseas under an exception in APP 8.2.

There is similar deemed liability for credit providers who disclose credit eligibility information in specified circumstances to certain bodies without an 'Australian link'[10] but there is no deemed liability for credit reporting bodies who are not permitted to disclose credit reporting information unless certain exceptions apply. Those exceptions are limited and

7 *Privacy Act 1988* (Cth), s 26WQ(3).

8 Section 16C, *Privacy Act 1988*.

9 *Privacy Act* 1988 (Cth), s 26WC; Although this is the position under the legislation, curiously, the Explanatory Memorandum to the bill introducing the NDB Scheme appears to suggest that s 26WC and s 16C will operate in the same way, when in fact, the latter contains a critical caveat to the effect that where the APPs apply to an overseas recipient of personal information, the disclosing entity will not be deemed liable. In contrast, the drafting of s 26WC indicates that a disclosing entity is liable for any breach of the NDB Scheme by an overseas organisation, regardless of whether the overseas recipient is subject to the APPs. Interestingly, the Explanatory Memorandum does not provide an explanation for this distinction between the two provisions.

10 Defined in s 5B of the *Privacy Act 1988*.

in most cases require that the party receiving the information has an 'Australian link'.

Although the OAIC recommends that where a single data breach involves multiple entities, the entity with the most direct relationship with the affected individuals should make the notification, if an overseas recipient of information disclosed by you suffers a data breach, keep in mind that you will be deemed liable for any failure to notify that breach.

It may still be appropriate for the overseas recipient to notify, depending on who has the closer relationship with affected individuals, but you should make sure that you retain appropriate oversight and input into the assessment of the breach, what the notification contains and how it is carried out.

Importantly, if no assessment or notification is undertaken when required, all of entities involved may be taken to have breached those requirements. In light of that it is worth looking in a little more depth at how you should consider responding to the uncertainty of a data breach involving jointly held information.

6 Data breaches involving jointly held information involve an additional layer of complexity.

When will you hold information?

For the purposes of the NDB Scheme, an entity will be considered to 'hold' personal information if it has possession or control over the relevant record,[11] that is where it has a right or power to deal with the record. This is not limited to physical possession.

This means you cannot simply avoid your obligation to notify under the NDB Scheme by outsourcing your data storage to a third party.

When will you *'jointly'* hold information?

Information will be held jointly where two or more entities hold the same record of personal information.

There is an important difference between jointly held data and newly created records that are derived from mutually held information.

This distinction is best demonstrated by an example given by the OAIC in its *Data breach preparation and response* guide. In this hypothetical scenario, a client company provides a market research firm with the personal information of individuals for a focus group. The information is provided in circumstances where contractual arrangements mean that the client retains control over how the information is used.

At this point in time, the personal information is jointly held between the client and the market research firm.

Following the focus group session, the market research team asks the focus group attendees whether they would like to participate in future research projects which they facilitate. All participants give their consent to have their personal information held by the market research company to be contacted for future research opportunities. The market research firm creates a new record containing this information.

This is a new record that is separate from the information that was held jointly by the client and the market research firm.

This new record is not *'held jointly'* for the purposes of the NDB Scheme, even though the personal information may be identical to that which is held jointly. As such, to the extent the new record is breached, only the market research firm will be responsible for notifying in respect of the new records, unless of course, the contractual arrangements stipulate that the client has the right or power to deal with newly created records.

Practically, this means that you should very carefully consider how different categories of data are dealt with in agreements, including by identifying which data you do have rights to deal with and when a newly created records will be out of your control.

Who should undertake the assessment and notification in relation to jointly held information?

The new scheme does not prescribe which entity should assess and/or notify,[1] allowing entities that hold information jointly to tailor their assessment and notification arrangements to accommodate their particular customer and contractual requirements.

Although the OAIC suggests that the entity with the most direct relationship with the individuals at risk of serious harm will often be best placed to notify, there may be situations where the OAIC's suggested approach isn't the preferred response from a commercial perspective (for example, where the system involved is so complex that the system host will be best equipped to deal with any further queries post-notification).

It is important to consider these issues in advance and to ensure that both parties are aligned as to who should assess and who should notify. In some circumstances, the parties might prefer that the entity that undertakes the assessment is different to the entity that notifies.

11 See *Data breaches involving more than one entity* in Part 4 of the OAIC's *Data breach preparation and response guide*

Top tips for dealing with jointly held information

1. Be careful not to rely too heavily on other organisations to carry out an assessment or make a notification in the absence of appropriate oversight. Ensure that you have clearly communicated the responsibilities of each entity holding that information in the event of a data breach (ideally by drafting this into your new and existing contractual arrangements), prior to any incident taking place. This will save any confusion and potential miscommunication in the aftermath of a significant data breach involving several entities across a number of possible locations.
2. In deciding how to allocate responsibility for undertaking an assessment and notifying the OAIC and affected individuals, weigh up all of the possible risks and benefits associated with the responsibility of notifying. Consider:
   - Who would be the 'public face' of the breach – are you or the other party likely to receive inquiries?
   - Who would affected individuals expect the notification to come from?
   - Who has the most direct access to the underlying systems that would be affected? Consider which entity will be best able to undertake the assessment and would be best placed to provide relevant and accurate information.
   - Is one party better resourced or more able to undertake the assessment or notification?
   - Who will be responsible for the costs of assessment and notification?
   - Who will be best placed to handle additional queries post-notification from the OAIC or affected individuals?
   - Do you or the other party have any additional notification obligations? For example, under continuous disclosure requirements or overseas data breach notification regimes.
3. Your contractual arrangements should contemplate:
   - a requirement that other parties be informed where one party suspects a data breach involving jointly held information has occurred;
   - the process for conducting an assessment where it is suspected that a data breach has occurred;
   - who should undertake an assessment of a suspected data breach in particular circumstances;
   - where an eligible data breach has occurred, who is responsible for notification to the OAIC and affected individuals; and
   - a right to review and/or sign-off on any data breach statement prepared for the OAIC and individuals whose information was involved in the data breach.
4. Other issues you may want to consider include:
   - If another party is responsible for the assessment and/or notification under the NDB Scheme, how might you ensure this has actually occurred?
   - What will happen if another party undertakes an assessment of the data breach and considers that notification is not required, but you disagree (or vice versa)? How might you resolve this stalemate?
5. Where the OAIC decides to review a data breach involving information you held jointly, it is important that you can demonstrate the steps taken to ensure compliance with the NDB Scheme. This might include any documentation prepared for the purposes of complying with the notification regime, any internal processes or procedures, and any correspondence with the entity responsible for notification at the time of the breach.

With the NDB scheme still in its infancy, it remains to be seen how bullish the OAIC will be in its pursuit of organisations that do not comply with it. That said, the considerable public outrage in response to the Cambridge Analytica Facebook scandal shows that privacy is clearly on the public's radar. If organisations want to retain the public's trust they should comply fully with the NDB scheme, not only because it is the law, but because it is what consumers are coming to expect.

Valeska Bloch is a partner in the Technology, Media and Telecommunications group at Allens.

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)