CAMLA COMMUNICATIONS LAW BULLETIN

Communications & Media Law Association Incorporated Volume 35, No 3. September 2016

An Update on Privacy Tort Reform with Professor Barbara McDonald

Tim Senior of Banki Haddock Fiora interviews Professor Barbara McDonald

Barbara McDonald is a Professor at the Faculty of Law at the University of Sydney and a Fellow at the Australian Academy of Law. She recently served as a Commissioner of the Australian Law Reform Commission (ALRC) where she headed the Inquiry into Serious Invasions of Privacy in the Digital Era.

Tim Senior is a specialist media lawyer at Banki Haddock Fiora, who regularly advises some of Australia's largest broadcasters and publishers.

TS: Professor McDonald, we are excited to hear your thoughts about developments in privacy tort reform since your ALRC report was published in 2014. It was observed by Gleeson CJ in *ABC v Lenah Game Meats Pty Ltd (2001) 208 CLR 199* that 'there is no bright line which can be drawn between what is private and what is not'. What does the concept of privacy mean to you?

BM: A surprisingly difficult question. I may now be too imbued with legal discussions - and the various uses to which the concept of privacy has been put in legal contexts – to separate out an ordinary use of the term. Essentially I think privacy refers to the state of keeping one's body and thoughts, aspects of one's life and information about oneself behind certain boundaries. These boundaries may be self-imposed or arise from expectations relating to our interactions with others in our private or public lives. In its 2008 Report For your Information: Australian Privacy Law and Practice, the ALRC noted four concepts of privacy: information privacy, bodily privacy, privacy of communications and territorial privacy (paragraph 1.31). This is a useful summary and directed to key privacy interests. In the 2014 Report we did not attempt to define privacy but rather concentrated on what test the law should use to determine whether particular information or activities should be characterised as private.

TS: The ALRC and recent New South Wales Standing Committee inquiries focused on the impact of

CONTENTS

digital or technology related invasions of privacy. In what way do such privacy breaches most commonly occur, and do you think they are on the increase?

BM: The two types of invasion of privacy that we concentrated upon were invasions by intrusion upon a person's physical or informational privacy and by the unwanted dissemination of private information. New technologies make both types of invasion easier and more intrusive or more damaging. New technologies from phones to drones to spyware allow instant or remote or automatic surveillance and recording of people, and their activities, movements, and communications with others. The internet enables widespread and almost uncontrollable aggregation and dissemination of private information. In our Inquiry we heard from people concerned with neighbourhood security cameras, public CCTV cameras, aggregation of data for commercial purposes, surveillance by activist groups, media intrusions and revelations, and the increasing phenomenon of "revenge porn", harassment and bullying by unwanted online revelations of private information.

Essentially I think privacy refers to the state of keeping one's body and thoughts, aspects of one's life and information about oneself behind certain boundaries.

TS: A statutory cause of action for invasion of privacy does not presently exist in Australia. In the UK and other jurisdictions, causes of action for serious invasions of privacy have developed through the common law, including via the extension of the equitable action for breach of confidence. Although there have been some cases in Australia where an action for breach of confidence has been brought to redress an invasion of privacy (for example *Giller v Procopets [2008] VSCA 236* and *Wilson v Ferguson [2015] WASC 15*), why hasn't the law here developed in the same way? Are we just waiting for the right case to come along?

BM: To a certain extent we are waiting for the right case to come along but it needs more than just a fact situation to arise for the common law to develop: it needs litigants and lawyers prepared to take a case to trial and through the appeal process, as well as courageous judges, for new law to be made and developed. There is some anecdotal evidence that litigants prefer to rely on settled principles such as breach of confidence if they can while media defendants would prefer to settle meritorious claims than have new law on privacy develop in the courts. We are a smaller population than the UK so perhaps we don't see the volume of case law that allows law to develop, although NZ courts in a smaller country with a similar legal heritage have shown their independence in fashioning a new tort. We also do not have a Human Rights Act such as the UK 1998 Act nor a Bill of Rights such as in NZ which have underpinned the developments in both of those countries.

TS: There have been a number of recent inquiries into the adequacy of existing remedies for breaches of privacy, including the ALRC inquiry you headed. Each of those inquiries has supported the enactment of a statutory cause of action for serious invasions of privacy, and yet there have been no changes to the law. Why do you think that is? Does it just come down to a lack of appetite from government?

BM: Yes I think so, but also from ignorance of what is being proposed. All statute law depends on political interests and priorities. That entails getting at least a modest consensus for change, and dealing with powerful lobby groups which may want to block change. Governments listen to business interests and some have made a case that they are already overregulated on privacy. They are usually referring in fact to the data-protection regimes such as in the *Privacy Act 1988* which does regulate the collection and storage and dissemination of some personal information for certain entities or under regimes governing state and territory government entities. The statutory cause of action would have a different context and would entail positive conduct that invades others' privacy in certain ways. Governments are often reactive and it may only be when there is an egregious case for which there is no existing remedy that a government will show interest in responding to a public outcry. Legislators are also reluctant to enact laws if they are uncertain as to how they will operate and whom they will affect: that is why we tried in the ALRC Report to be as specific as we could in our recommendations and why we limited the proposed cause of action to the two most troublesome types of invasions of privacy and to intentional or reckless conduct.

TS: Does Australia actually need a statutory cause of action for invasion of privacy? What's wrong with the current protections and remedies that exist, for example the State and Commonwealth information privacy legislation and common law actions like breach of confidence?

BM: There are numerous gaps in the protection currently offered by information privacy legislation (it only affects certain entities) and by common law actions which were developed with privacy as only an incidental interest to be protected: we set these out in Ch 3 of our Report. Importantly the common law makes it difficult to claim compensation for even acute distress which is the most common consequence of an invasion of privacy.

TS: Do you see any risks or potentially negative consequences in introducing a blanket statutory cause of action for serious invasions of privacy? For example, opponents of a privacy law suggest that it may have an adverse effect on freedom of speech, including the media's ability to report stories of legitimate public concern, or lead to a flood of UK style super-injunc-

tions. What measures could be included in a statutory cause of action to ensure a fair balance between the protection of privacy and free speech?

BM: Yes I think we first need to avoid a statutory tort which is drafted in too general, unspecific, terms. We also need to build strong protection of these other interests into the design of the action itself which is what we did in our Report. We recommended that a serious invasion of privacy not be actionable unless the court was satisfied that the public interest in protecting the claimant's privacy outweighed any countervailing public interest. In other words countervailing public interest such as freedom of speech and the freedom of the media would have to be determined at the outset of the action rather than merely as a defence. It was disappointing that many, although not all, media interests were so intent on blocking and disparaging any discussion of further privacy protection that they did not recognise the benefits to their interests of this recommendation. Nor that legislation can have the real advantage of making specific protection for countervailing interests in a way that may not happen in common law development. Further recommendations that would enhance the protection of media interests under existing law were made in Chapter 13.

TS: Speaking of super-injunctions, what's your view on the recent judgment of the UK Supreme Court in the matter of *PJS v News Group Newspapers Ltd [2016] UKSC 26*, in particular the Court's decision to maintain the injunction notwithstanding that the identity of the appellant had been widely published and was known to many people in other jurisdictions? More generally, what do you think about the way privacy law has developed in the UK?

BM: On the *PJS* case, one of the interesting contrasts between privacy and confidentiality is that although the latter might be lost by information coming into the public domain, this is not necessarily the case with information that is private. For example, a picture or footage of someone naked in a shower, taken against her wishes, will always be "private" in nature unless she chooses to disclose it. It may not lose its private nature because it's been passed around by her boyfriend of the time or published on the internet and there should not be carte blanche to everyone to continue to invade her privacy by publishing the footage to new audiences, although obviously the fact that it has been published may affect causation and the level of compensation. Privacy invasions may be cumulative and ongoing. Legislation could consider a first publication rule as exists now in UK defamation law but this would not protect everyone who renewed the invasion. Interestingly, privacy litigation in the UK seems to have developed rapidly but become relatively settled in the very short time since the Naomi Campbell case in 2004. While compensation is modest (in contrast to the large sums given in settlement of phone-hacking claims), there has been some impact on the amount of gossip and personal trivia the media now publish. I have not heard of it restricting the publication of matters of *real* public importance. I am told that their broad *Data Protection Act* is providing a steadier stream and basis for action than the privacy cause of action. There are still a number of legal oddities – for example, the characterisation of the equitable claim as a tort, without full consideration of the implications of this - but English judges and academic commentators are far less concerned with precedent and classification than their Australian counterparts.

TS: The New South Wales Standing Committee released its report into remedies for serious invasions of privacy in March this year. The report recommended that a statutory cause of action be introduced in New South Wales based on the model set out in the ALRC 2014 report. The State government has until September this year to respond to the Standing Committee's report. What do you think the impact will be if the government adopts the recommendation and enacts a privacy law in New South Wales? Will the other States and Territories follow suit or will New South Wales become the privacy capital of Australia? How would you recommend preventing the possibility that we could end up in a situation, similar to the PJS case in the UK, where someone's identity is supressed in New South Wales because of the new privacy legislation, but is publishable and known in other States and Territories that have not enacted the same law?

Governments are often reactive and it may only be when there is an egregious case for which there is no existing remedy that a government will show interest in responding to a public outcry.

BM: The ALRC took the view that a nationwide federal action would be preferable to ensure both equal protection for all Australians and also, importantly, consistency for business and other entities across the country. Inconsistent legislation would create complex and therefore expensive jurisdictional and practical issues. Separate state Acts would reflect the bad old days before the uniform Defamation Acts of 2005. South Australia may be the state most likely to follow suit if New South Wales takes the lead because of the recent report by the South Australian Law Reform Institute supporting an action and because South Australia has often led the way on social reforms. On the issue of suppression orders or injunctions in different states, courts will not grant injunctions that are futile but I also assume that a NSW statute could be given some extraterritorial operation for media and internet organisations before a court in NSW. Again, invasions of privacy in one place or time may not cease to be invasions just because they have also occurred in other places or times.

TS: Thanks for your thoughts, Professor McDonald.

Cyber Resilience: Managing Cyber Risk for Sustainable Prosperity

David Gerber, Partner, Clayton Utz and Lachlan Gell, Lawyer, Clayton Utz consider ASIC's recent focus on cyber risk management and cyber resilience

INTRODUCTION

On 21 April 2016 the Prime Minister, the Hon Malcolm Turnbull MP, launched Australia's new $230 million Cyber Security Strategy. Although the strategy has a focus on protecting Australian public sector organisations from cyber threats, it also addresses the importance of cyber security and cyber resilience in the private sector. The strategy emphasises that it is the responsibility of businesses themselves, and not the government, to ensure that they are able to manage effectively cyber security threats. Under the heading 'raising the bar', the strategy proposes that: "[s]elf-regulation and a national set of simple, voluntary guidelines co-designed with the private sector will help organisations improve their cyber security resilience." [1]

The strategy emphasises that it is the responsibility of businesses themselves, and not the government, to ensure that they are able to manage effectively cyber security threats.

To this end, the Government proposes to introduce an online "cyber threat sharing portal" for all businesses to share and collaborate on threats. It will also provide voluntary "health checks" to ASX 100 listed businesses, enabling them to better understand their cyber security status and how they compare to similar organisations.

Although the strategy stresses the importance of organisations strengthening their cyber defences and sharing information, it does not provide detail as to how cyber resilience ought to be improved. Over the last year, the Australian Securities and Investments Commission (**ASIC**) has, however, released reports which give this guidance. ASIC's reports explain how businesses can review and update their cyber-risk management practices.

This article provides an overview of ASIC's focus on cyber risk and cyber resilience. It sets out a step-by-step guide to assessing cyber resilience, summarises ASIC's practical guidance and lists questions that a board of directors may wish to ask when reviewing the organisation's risk management framework. It also examines briefly the government's recent proposal to introduce a mandatory cyber breach reporting regime. The authors conclude that cyber security and resilience will be key to sustainable prosperity in the information age.

CYBER RISK AND THE IMPORTANCE OF CYBER RESILIENCE

Every day we create and share information electronically as a fundamental part of doing business. The risks of doing so are numerous and increasing. They can lead to loss of data and serious privacy breaches, system shutdowns or even electronic blackmail and extortion. The impact of cyber risks can be significant - practically, legally and financially. Beyond the immediate costs to resolve cyber issues affecting systems and data, there can be profound impacts on reputation and potentially liability to third parties.

There is a growing recognition of the widespread risk to Australian businesses of all sizes of cyber-attacks and data breaches.[2] ASIC has released reports aimed at increasing awareness among Australian businesses of cyber risk and the importance of cyber resilience. These reports also indicate that the issue of cyber risk is now firmly on the regulatory agenda and should be front of mind for companies and their directors in almost all sectors of the economy, but most notably those regulated by ASIC's licensing regimes.

WHAT SHOULD ORGANISATIONS BE DOING TO MANAGE CYBER RISK?

In March 2015, ASIC released a report titled "Cyber Resilience: Health Check".[3] The report recommended that regulated entities review and update their cyber-management practices. ASIC suggested a health check on "cyber resilience" which ASIC defines as the ability to prepare for, respond to and recover from a cyber-attack.

The "health check" encourages businesses to take a number of specific actions, including:

1. to identify and monitor cyber risks;
2. to actively monitor trends in cyber risks and adapt to new cyber risks as they arise;
3. to let their customers and clients know if their personal data has been compromised;
4. to take responsibility for improving their cyber resilience;
5. to consider using the NIST Cybersecurity Framework[4] to help the business develop cyber resilience

1 Commonwealth of Australia, Department of the Prime Minister and Cabinet, *Australia's Cyber Security Strategy* (April 2016), p. 35.

2 Commonwealth of Australia, *Financial System Inquiry Final Report* (November 2014), pp. 268-269.

3 Australian Securities and Investments Commission, Report 429 *Cyber Resilience: Health Check* (19 March 2015).

in a proportional way, particularly where their exposure to a cyber-attack may have a significant impact on financial consumers, investors or market integrity;

6. to report cybercrime and cybersecurity incidents to relevant government agencies;
7. to consider using a CREST Australia[5] approved member organisation to help test existing IT systems, processes and procedures to ensure that they respond well to cyber risks;
8. if it is regulated by ASIC, to mitigate cyber risks by, at a minimum, implementing the ASD's[6] four highest-ranked mitigation strategies;
9. if it is regulated by ASIC (and particularly, if a licensee), to address cyber risks as part of their legal and compliance obligations - including risk management and disclosure requirements;
10. if it is an AFS licensee, to review the adequacy of their risk management systems and resources to address cyber risks; and
11. depending on a company's risk profile, consider taking out cyber insurance.

In March 2016, ASIC issued a further report titled "Cyber resilience assessment report: ASX Group and Chi-X Australia Pty Ltd".[7] The report presents the findings of ASIC's cyber resilience assessments of Australia's major financial infrastructure providers. It also provides some examples of cyber resilience good practices implemented by a wider sample of organisations operating in the financial services industry.

In conducting its formal assessment of the ASX Group and Chi-X, ASIC identified the following practices as the most resilient or "adaptive" across the organisations:

- established information security policies are periodically reviewed and updated;
- cyber security roles are defined, communicated and understood at the senior management level;
- legal and compliance obligations are understood and managed;
- response and recovery plans are managed, communicated and tested on a periodic basis; and
- cyber events are communicated within the organisation to ensure ongoing awareness of threats.

The 2016 report also encourages organisations to recognise the growing threat of cyber security, and improve their cyber resilience preparedness. It encourages them to adopt a number of cyber resilience good practices. These include:

- ongoing board engagement with cyber strategy and board ownership of cyber resilience;
- governance practices that are responsive to a rapidly changing cyber risk environment;
- cyber risk management driven by routine threat assessment of both internal and third party sources such as cloud-based service providers;
- collaboration and information sharing with other industry members, security agencies and law enforcement; and
- creating an organisational culture of cyber awareness through training programs.

CYBER GUIDANCE

ASIC is also proposing to issue guidance on cyber resilience, which would include the following key concepts:

- the attention of the board and senior management is critical to a successful cyber resilience strategy;
- the ability to resume operations quickly and safely after malicious cyber activities is paramount;
- providers should make use of good-quality threat intelligence and rigorous testing;
- cyber resilience requires a process of continuous improvement; and
- cyber resilience cannot be achieved by a financial market provider alone, it is a collective effort of the whole ecosystem.

cyber security and resilience will be key to sustainable prosperity in the information age

ASIC expects that the Cyber Guidance will be finalised in the second half of 2016.

KEY QUESTIONS FOR AN ORGANISATION'S BOARD OF DIRECTORS

Of particular interest is the emphasis that ASIC places on the responsibility for cyber resilience as an issue for an organisation's board of directors and senior management. ASIC has encouraged company officers to address the following key questions when reviewing their risk management frameworks:

1. Are cyber risks an integral part of the organisation's risk management framework?
2. How often is the cyber resilience program reviewed at the board level?
3. What risk is posed by cyber threats to the organisation's business?
4. Does the board need further expertise to understand the risk?

4 The NIST Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity issued by the National Institute for Standards and Technology.

5 Council of Registered Ethical Security Testers Australia.

6 Australian Signals Directorate.

7 Australian Securities and Investments Commission, Report 468 *Cyber resilience assessment report: ASX Group and Chi-X Australia Pty Ltd* (7 March 2016).

5. How can cyber risk be monitored and what escalation triggers should be adopted?
6. What is the people strategy around cybersecurity?
7. What is in place to protect critical information assets?
8. What needs to occur in the event of a breach?

By placing the ultimate responsibility of cyber risk management on the officers of a business, this regulator has made it clear that cyber resilience is not simply a matter of good practice but, essentially, is one of regulatory compliance.

this legislative reform is expected to increase further the focus on cyber risk management

MANDATORY BREACH NOTIFICATION REGIME

Although not mentioned in the Cyber Security Strategy, ASIC's reports are timely given the Government's recent proposal to introduce a mandatory data breach notification scheme for entities regulated by the Privacy Act. The proposed scheme will likely mean that significant data breaches receive heightened attention from both the Office of the Australian Information Commissioner (**OAIC**) and ASIC.

Organisations which are subject to the *Privacy Act 1988* (Cth) are currently required to protect personal information from misuse, interference and loss, unauthorised access, modification and disclosure under Australian Privacy Principle 11. However, they are not subject to a mandatory data breach notification requirement under the Privacy Act. They are obliged to minimise the likelihood that personal information within their possession could be compromised. The legislation does not yet require them to notify an individual or agency in the event of an actual or suspected security breach. This is expected to change.

In December 2015, the Federal Government released a discussion paper[8] and an exposure draft of the *Privacy Amendment (Notification of Serious Data Breaches) Bill 2015*. The Bill, if passed, will require certain entities to notify "serious data breaches" to affected individuals and the Australian Information Commissioner as soon as practicable. A "serious data breach" is one that creates a "real risk of serious harm" to the affected individuals. This includes harm to reputation, economic and financial harm, and may include physical, psychological and emotional harm. Guidance is expected to be issued by the OAIC to help businesses comply with the requirement to identify where "serious data breaches" have occurred.

Under the proposed Bill, an organisation would be required to notify the Commissioner of the details of the serious breach; the compromised information; and any remedial steps that victims should take. Businesses that fail to comply with the provisions would risk enforcement action including civil penalties for serious or repeated infringements. Further, a business will also be found to have failed to comply with the notification obligations if it was not aware of a serious data breach, but reasonably should have detected it.

There is much to be said for the introduction of mandatory data breach notification legislation.[9] If an organisation has suffered a serious data breach, notification will give people the opportunity to reduce the impact of the breach (e.g. by cancelling credit cards or changing account passwords). It should also increase public confidence in the handling of consumer information as organisations are compelled to improve their data security procedures and policies.

For an organisation that has suffered a data breach, mandatory notification gives rise to potential reputational risk and cost. Put simply, when an organisation is faced with regulatory investigations and is obliged to take steps to notify customers of a data breach, it is likely to incur significant legal and other costs. This may include costs to defend regulatory action on behalf of a class of affected individuals or, depending on the circumstances of the data breach, potentially even a class action. They will likely also face increased media and other public scrutiny. Therefore this legislative reform is expected to increase further the focus on cyber risk management. It may also drive the market for cyber risk insurance policies. An individually tailored cyber insurance policy can be a valuable tool for managing these risks and costs.

CONCLUSION

ASIC has cautioned that the 'weakest link' is often the real measure of an organisation or industry's cyber resilience. The regulator suggests that organisations ensure good practices are in place for assessing cyber risk and driving continuous improvement.

Clearly, both ASIC and the government expect that an organisation's cyber resilience framework must evolve continuously to cope with the dynamic and unpredictable nature of cyber threats. It is therefore essential for businesses in the private sector to have a long-term and comprehensive commitment to cyber resilience to deal with the issue of cyber threats.

Like many business opportunities, cyber carries with it some risk. The organisations which manage most effectively their cyber security and build and maintain cyber resilience, will be best placed to extract the value from developing or disruptive technologies in a sustainable way.

DAVID GERBER (Partner) and LACHLAN GELL (solicitor) practise in the Insurance and Risk group at Clayton Utz.

8 Commonwealth of Australia, Attorney-General's Department, *Discussion paper - Mandatory data breach notification* (December 2015).
9 See Smyth, Sara N, "Does Australia Really Need Mandatory Data Breach Notification Laws - And If So, What Kind?" (2013) 22(2) *Journal of Law, Information and Science* 159.

Developments in Data Driven Law: A Discussion With Peter Leonard

Eli Fisher, co-editor, interviews Peter Leonard, Partner, Gilbert + Tobin.

INTRODUCTION

Eli Fisher, co-editor, sits down with Peter Leonard, the head of Gilbert + Tobin's Data and Content practice. Peter's primary focus has become data driven businesses and business ventures, including data analytics, privacy compliant data sharing, cloud computing, e-health and internet of things deployments. He also advises in relation to communications and e-payments regulation, privacy, interception and data protection. Peter is Best Lawyers' Sydney Technology Lawyer of the Year 2016 and he has been the Communications Alliance's Australian Communications Ambassador. He is currently the chair of the Law Council of Australia's Media and Communications Committee.

We discuss recent developments in privacy and data protection law, including those in connection with the *Grubb v Telstra* litigation; the *Privacy Amendment (Notification of Serious Data Breaches) Bill 2015* addressing mandatory data breach notification; proposed development of a privacy statutory cause of action; and the ongoing Productivity Commission inquiry into data use and availability in Australia.

Privacy and data policy has taken on enormous importance in recent years, with the ALRC publishing its report on Serious Invasions of Privacy and the revision of the *Privacy Act* and introduction of the Australia Privacy Principles, each in 2014. This has occurred at a time where collecting, analysing and exploiting unprecedented volumes and range of data has become a key business driver for many large businesses and there has been explosive growth in the range of devices, applications and services collecting personal data and tracking movement and behaviour of individuals. This has occurred within a legal environment of continued uncertainty as to the range of information about individual's interactions with devices and services that should be considered personal information, very limited protection afforded by post *Ice TV* Australian copyright law for databases and other computer-generated works and nascent application of equitable doctrines protecting confidential information to data sets that are shared under access controlled conditions. While initial focus was on privacy concerns, debate about big data has moved to encompass novel issues of legal liability arising from reliance upon artificial intelligence, liability for wrong decisions correctly made on the basis of incorrect or incomplete data, discrimination by algorithmic decision-making and use of data as a shield and a sword in private litigation. With the Productivity Commission's ongoing review of data availability and use in Australia and focus upon fraudulent misuse of data in the financial sector, lawyers and clients from a range of industry sectors can expect that public policy and legal developments in this area of law will not be far from the Government's attention.

In the circumstances, we are extremely grateful to have Peter's insights.

EF: Peter, thanks for contributing to the CLB. It seems that everywhere we look there is a new development in the laws surrounding privacy and data protection. That is no doubt justified given the way personal information has become a currency in the digital era.

Privacy law has never been dull or slow, but I can't think of a time where it has moved at this velocity.

PL: We all know that Mark Zuckerberg of Facebook said that privacy is dead. For a corpse, privacy is kicking a lot! Privacy law is not well understood by Australian businesses. Even Government agencies that should know better mess it up: look at the recent Australian census crisis which started with a very light-on privacy impact assessment and the inadvertent disclosures by the Department of Immigration. The Australian media also love a bad corporate behaviour privacy story: these stories are easy to tell and readily understood. Many 'privacy breach' or 'privacy invasion' stories run even where there is no relevant breach under Australian law. Also, privacy means different things to different consumers. Some see invasions of privacy everywhere and then are very vocal about it. There are deep divides about privacy within the Australian public, which is fragmented along cultural, inter-generational and sometimes socio-economic lines. The much commented upon fact that Millennials share intimate details of their private and social lives with each other doesn't make them any less zealous in defending access to information that they regard as private and sensitive: have you tried to get passwords from your teenage kids, or even an intelligible description of which services they are using this week? Privacy law has never been dull or slow, but I can't think of a time where it has moved at this velocity.

EF: I suppose one of the most interesting developments in privacy jurisprudence is the exploration of the meaning of "personal information" – perhaps the central theme of the Privacy Act – currently being undertaken through the Grubb v Telstra litigation. Can you walk us through it?

PL: In May 2015, the Australian Privacy Commissioner, Mr Timothy Pilgrim PSM found that Telstra had breached the *Privacy Act 1988* (Cth)

by failing to provide Mr Grubb with access to requested 'metadata' relating to his use of Telstra mobile services, including geo-location information relating to movement of the phone and call related data. This data was collected and held by Telstra in various databases for various purposes, some purely technical e.g. operation of the network and monitoring its performance. In December 2015, the Administrative Appeals Tribunal overturned the earlier determination by the Australian Privacy Commissioner granting journalist Ben Grubb access to certain data relating to his use of Telstra mobile services. The decision of the Administrative Appeals Tribunal was then appealed by the Australian Privacy Commissioner to the Full Federal Court, with the appeal hearing taking place just before this CLB went to print.

Just because a particular proposed application is legal, considered ethical and in line with corporate social responsibility principles, and likely to be acceptable to that section of the public with which a business proposes to deal, does not mean that a business should go straight ahead and engage in that practice

It was not in dispute that Mr Grubb as an individual could be linked to relevant network data relating to use by Mr Grubb of his mobile phone, by a multi-step process that involved significant labour input and manual matching to trace and then match records held in multiple databases in Telstra's systems. What was in dispute was whether Mr Grubb's identity could reasonably be ascertained from the relevant network data. Before the Privacy Commissioner this was treated as a question as to the reasonableness of the multiple steps required to link the network data through to Mr Grubb as an individual. On appeal, that issue was again contested, but in addition there was extensive analysis as to whether relevant network data was information 'about an individual', or information about a device that incidentally related to an individual. This might initially appear a somewhat esoteric debate, but consider the arriving world of internet of things (IoT): many sensor devices collect information in the course of provision of a service provided to a consumer (for example, a remotely controlled climate control system in a smart home), but is this information about an individual merely because the customer was an individual?

The Privacy Commissioner found that although Mr Grubb's identity was not apparent in relevant Telstra databases where relevant metadata was held, the device identifiers, IP addresses and other transactional information there held could be traced through from mobile tower records to operational and network databases and on to personally identifying databases (in particular, the Telstra customer billing database). In fact, Telstra regularly complied with requests by law enforcement agencies for lawful assistance as to the use of mobile phones by persons of interest by undertaking the same tracing and matching processes.

In the AAT Deputy President S A Forgie stated that where an individual is not intrinsically identified in information, a two-step characterisation process should be applied. The first step is determining whether relevant information is "about an individual." The second step is working out whether an individual's identity "can reasonably be ascertained from the information or opinion". If relevant information is not "about an individual," that is the end of the matter. But if information is information "about an individual," the second step must be applied. The Tribunal then reasoned: "The data is all about the way in which Telstra delivers the call or the message. That is not about Mr Grubb. It could be said that the mobile network data relates to the way in which Telstra delivers the service or product for which Mr Grubb pays. That does not make the data information about Mr Grubb. It is information about the service it provides to Mr Grubb but not about him".

EF: With respect to the Tribunal, it's a surprising decision. What are your thoughts about it, and what are its implications?

PL: The reasoning of the Tribunal is novel and perhaps surprisingly, does not include reference to relevant analogous cases in England and New Zealand. The Full Federal Court might be expected to be directed to a broader range of authorities than was considered before the Tribunal and may well reverse the Tribunal's decision.

In my view there is no bright line to be found between what is information about an individual who is reasonably identifiable and what is not. Usually the issue should not arise because good privacy practice is to be overly broad in characterising personal information. Australian privacy law is not particularly onerous. Often privacy compliance can be assured and built-in to the design of a product or service (so-called 'privacy by design') without undermining the business case for a particular data application. Ben Grubb's application was for access to data, not a complaint that Telstra was collecting and using relevant information to provide a service to Mr Grubb. In any event, privacy is not an area where boundaries of what is or is not legal should always be determinative of business activity. Just because a particular proposed application is legal, considered ethical and in line with corporate social responsibility principles, and likely to be acceptable to that section of the public with which a business proposes to deal, does not mean that a business should go straight ahead and engage in that practice. As already noted, the community is not homogenous and it is reasonable to tailor products and benefits for sharing of information to suit particular segments.

But these products will also be scrutinised by privacy advocates that are good at briefing the media. Trying to generalise as to consumer expectations of privacy when there are deep divides about privacy within the Australian public is a challenging task. And trying to deal with a diversity of opinions as to good data ethics is even more problematic. This is an area where caution is often desirable. Just ask the Australian Statistician about his experience in dealing with concerns about the Australian Census!

EF: There's also been another attempt to introduce mandatory breach notification requirements in the *Privacy Act*. *The Privacy Amendment (Privacy Alerts) Bill 2013* (Cth) was a similar attempt, but which did not progress to legislation, lapsing without Senate consideration when that parliament was prorogued for the election. The recent Bill, the *Privacy Amendment (Notification of Serious Data Breaches) Bill 2015*, seems like it may have better prospects. What are your thoughts?

PL: The Australian Government in December 2015 invited public comment on a draft serious data breach notification bill before legislation is introduced in Parliament in 2016. The draft Bill would require Government agencies and businesses subject to the *Privacy Act 1988* (broadly, any business doing business in Australia that had a global group annual turnover in excess of $AU 3 million) to notify the national privacy regulator and affected individuals following a serious data breach. The Privacy Commissioner received 110 voluntary data breach notifications in 2014-15, up from 67 notifications in 2013-14 and 61 in 2012-13. The Privacy Commissioner's enquiries into voluntary data breach notifications focus on the nature of a breach (such as the kind of personal information involved, and how the breach occurred), and the steps taken to contain the breach, mitigate harm to affected individuals, and improve security practices in future. However, the Privacy Commissioner does not have specific powers to deal with data breaches (as distinct from data breaches which constitute a breach of the APPs).

I would expect that this draft Bill will be revised and introduced into the current Parliament. There was significant support expressed in submissions as to the draft Bill, albeit qualified with issues as to scope and drafting. It is fair to say that some businesses and agencies covered by the Privacy Act 1988 ("APP entities") still don't appear to understand the importance of good information handling and reliable processes and practices of protecting information security, including consumer privacy. Given limited resources of the Australian Information Commissioner, mandatory data breach notification may be an appropriate discipline upon these less responsible APP entities.

In addition, further delay of any Federal statutory response increases the risk of pre-emptive State or Territory response. This might be grandstanding, but it might also be a fair expression of frustration as to slow progress of a Federal response and reflective of concerns of many businesses and government agencies that that consumer unease about new privacy affecting initiatives, including as to sharing of health related data and through deployment of IoT devices, may delay their uptake. I suggest that it is in the interests of governments and the business sector to promote consumer confidence in handling of consumer data. Consumer confidence requires openness of APP entities, including when things go wrong.

Also, a well-considered Federal Bill would be a good precedent for State and Territory based responses covering those entities that are subject only to State based privacy laws, in particular State and Territory government departments, agencies and state owned corporations. That noted, it would be unfortunate if those entities covered by State or Territory and Federal laws, in particular health service providers, were subject to two separate privacy breach notifications schemes each requiring notifications to affected individuals, but with differing standards or other requirements.

I would expect that this draft Bill will be revised and introduced into the current Parliament. There was significant support expressed in submissions as to the draft Bill

EF: There's also been yet another inquiry into the development of a cause of action for serious invasions of privacy. It's hard to think of any other area of law that has given rise to so many similar inquiries, which essentially reach very similar conclusions, to no effect whatsoever. Five inquiries in Australia have proposed that parliaments enact a statutory right to privacy in the last 8 years alone. What is your take?

PL: On 3 March 2016 the New South Wales State Parliament Standing Committee on Law and Justice released the findings of its Inquiry into Serious Invasions of Privacy in NSW, recommending that NSW introduce a statutory cause of action for serious invasions of privacy. The Committee went further to recommend a significant expansion of the powers of the NSW Privacy Commissioner to address claims of serious invasions of privacy. The NSW Privacy Commissioner, Dr Elizabeth Coombs, said "This is a win for those people who have had their privacy breached in unimaginable ways and then suffered further indignity in discovering that they had no right to recourse..."

Although the Australian Law Reform Commission in 2014 recommended the introduction of a federal statutory cause of action for serious invasions of privacy, that recommendation was roundly criticised by the Australian media as an undue fetter upon freedom of expression and effectively shelved by the Federal Attorney-General. The State recommendations raise the spectre of State and

Territory statute based causes of action with variants, inconsistencies and incomplete coverage, as is the case with surveillance device and tracking device regulation today. It is possible that this New South Wales initiative may re-ignite discussion as to a Federal approach. In the meantime, plaintiff's lawyers seek to shoehorn privacy infractions into the developing equitable doctrine of misuse of confidential information, with varying success in State courts. A number of 'revenge porn' cases, where estranged boyfriends have then published photos of videos of intimate active with their former girlfriends, have prompted the courts to extend the doctrine of misuse of confidential information in order to provide a remedy to understandably distressed plaintiffs. New statute laws now being introduced that specifically address such non-consensual publication of intimate material may stem that tide, but until such laws provide remedies across Australia we may expect continued litigation in this area.

There is a difficult balance to be found here and the Productivity Commission is first in to try to find that balance.

The potential for creative expansion of misuse of confidential information to fill the gap of absence of a tort or statutory cause of action for invasion of privacy was illustrated in early March 2016 by novel pleadings filed in the NSW Supreme Court by mining magnate Gina Rinehart, contesting such details as her weight, whether her father cheated at tennis and the colour of her mother's hair, in her claim against Channel Nine and production company Cordell Jigsaw over the television broadcast of mini-series House of Hancock. Ms Reinhart sued for injurious falsehood, misleading and deceptive conduct and damages for breach of privacy, claiming she has a right "to live her life without being subject to unwarranted and undesired publicity, including publicity unreasonably placing her in a false light before the public". Among other remedies, Ms Reinhart sought an injunction preventing the DVD copy of the program being advertised as a "true story". This matter was recently settled without admissions. Such 'false light' claims seek to extend the reach of both defamation laws and the doctrine of misuse of confidential information to 'fill the gap' and create a right of seclusion for individuals in Australia.

EF: And lastly, what are your thoughts about the Productivity Commission's enquiry into Data Use and Availability?

PL: This is an important inquiry with a broad and challenging brief. On the one hand, Australian citizens have reasonable concerns as to personal information or other sensitive information about them entering into the public domain, being shared inappropriately or otherwise being used in ways that that are not transparent, open and understood and agreed. On the other, data flows should be facilitated as promoting business efficiency and consumer welfare. Data analytics and uses of data through IoT applications will often promote business efficiency and consumer welfare through any or all of reduced costs from higher asset utilisation, higher labour productivity, lower waste and improved supply chain logistics, businesses gaining new customers from improved product experiences and reducing the time to market for innovations. Also, many governments around the world, including the Federal government and State and Territory governments, have stated an intention to release public data sets wherever practicable. This commitment to open government data reflects policy that, because government data is collected at the expense of the public purse for the benefit of government in serving the public good, the default should be that this government data is released, non-exclusively and as 'open data'. But many government agencies resist opening up data, citing privacy concerns or concerns that data cannot be certified to be reliable and accordingly may be used inappropriately or in ways that expose government to legal liability. There is a difficult balance to be found here and the Productivity Commission is first in to try to find that balance.

Further, Australian copyright law provides very limited protection for databases and for computer-generated works, and fails to recognise or encourage intellectual and commercial investment in these types of works. In a digital context, databases and compilations are increasingly created through the joint efforts of multiple contributors, and the use of (new) technologies. A failure to protect commercially valuable works which are substantially computer-generated (as opposed to being the direct product of human effort) fails to recognise the use and adaptation of new technologies, and is a disincentive to the creation and dissemination of these works. Misappropriation of these works by third parties can cause significant damage to the owner of the works. Are developing equitable doctrines as to protection of confidential information up to the task of protecting an essentially non-proprietary asset, in the form of trade secret databases of business information? Many legal practitioners have concerns and think that statutory intervention may be necessary to supplement equitable doctrines, particularly given the central value of confidential business data to data-driven businesses. It does seem odd that the fastest growing asset class in Australia is not formally recognised by any existing head of intellectual property, or indeed formally recognised as property at all. But perhaps that is not surprising, given that we are just starting to recognise data management as a field of legal practice.

At this rate, by the time that it is widely accepted, we human technology lawyers may have been replaced by artificial intelligence, that can then devise their own governance free from our troubling interventions!

Battle of the Drones – Legal Issues for High Flyers

Sophie Dawson and Daniela Lai, Ashurst

Drones have quickly gone from being a science fiction-like futuristic concept to being an everyday device available in electronic stores at very reasonable prices. Consequently, they are being used domestically, commercially and by government organisations to an increasing extent.

This article discusses some of the key legal considerations to bear in mind when considering creative uses for drones. No doubt, there are many others that can come into play with specific uses.

1. INCREASING POPULARITY OF DRONES

Before delving into the legal technicalities, it is worthwhile to quickly discuss some of the uses to which drones are being productively put.

Google has recently trialled the use of drones for the delivery of packages. It is used by a Queensland farm on the Darling Downs as the testing ground for a drone delivery project which could see cost effective autonomous drones deliver medicines, gifts and other supplies to people in remote areas. According to media reports, the first person in the world to receive a delivery from a deliverable drone was a Warwick farmer called Neil Parfitt, who was delivered a package of Cherry Ripes[1]. Amazon has engaged in similar trials and, according to one report, has proposed that there be a "drones only" airspace between 200 feet and 500 feet above ground level.[2] Governments have also used drones around the world for military purposes.

Further, many real estate agents are now taking photographs of homes for sale using drones in order to cheaply obtain aerial shots for marketing purposes, and people are also using drones domestically for similar photographic purposes.

WHAT ARE THE KEY LEGAL ISSUES?

The key issues that arise in relation to drones include:

1. The Civil Aviation Safety Authority's (**CASA**) Regulations, in relation to remotely piloted aircraft;
2. Surveillance laws;
3. Privacy; and
4. The laws of trespass.

There are other laws of potential significance too, including nuisance and negligence. Those laws are outside the scope of this article.

1. CASA Regulations

The *Civil Aviation Safety Regulations 1998* (**CAS Regulations**) place restrictions on the operation of remotely piloted aircraft (**RPA**) such as drones.

Operations of RPA for commercial purposes will generally require certification for the business conducting the operation, known as a remotely piloted aircraft operator's certificate and a remote pilot licence for the pilot flying the drone. Amendments to the regulations which will come into effect on 29 September 2016 will allow RPAs which are considered to be lower risk, known as excluded RPAs, to have fewer restrictions such as not needing a remote pilot licence or remotely piloted aircraft operator's certificate. The regulations create new weight classifications for RPA where very small RPA weigh less than 2 kg, small RPA weigh between 2 to 25 kg, medium RPA weigh between 25-150 kg and large RPA weigh more than 150 kg.

Consequently, use of a camera attached to a drone is likely to be use of an "optical surveillance device" and care needs to be taken in every case to ensure that the applicable laws are complied with

Commercial operators flying very small RPAs will not require a remote pilot licence or operator's certificate. Operators flying very small RPAs must provide one notification to CASA at least five days before their commercial flight and operate by the standard operating conditions.

Private landowners are also exempt from needing a remote pilot licence or operator's certificate for operating a small RPA on their own land for certain purposes if they follow the standard operating conditions and none of the parties receive remuneration. Private landowners operating a medium RPA on their own land will be required to hold a remote pilot licence.

The standard RPA operating conditions include:

- an RPA must only be flown during the day and kept within visual line of sight;
- an RPA must not be flown higher than 400 feet;
- an RPA must be kept at least 30 metres away from other people;
- an RPA must be kept at least 5.5km away from controlled aerodromes;

1 Brisbane Times 29 August 2014 "Google drones tested in Queensland".

2 The Guardian 29 July 2015 "Amazon proposes drones-only airspace to facilitate high-speed delivery".

- an RPA must not be flown over populous areas such as beaches, parks and sporting ovals;
- an RPA must not be flown over or near an area affecting public safety or where emergency operations are underway without prior approval; and
- an operator must only operate one RPA at a time.

The operating of RPA without a required remote pilot licence or operator's certificate attracts a penalty of up to $9000.

The Privacy Act does not generally affect use of drones by individuals for personal or domestic reasons. This is, among other things, because the Act contains a carve out in relation to the non-business activities of individuals

2. SURVEILLANCE LAWS

Optical surveillance is regulated in Victoria, the Northern Territory, Western Australia and New South Wales. An Act has also passed but has not yet commenced in South Australia. Each jurisdiction which regulates optical surveillance has a prohibition on publication or communication of information obtained through unlawful use of an optical surveillance device. We have assumed for the purpose of this article that the recording equipment that can be included in drones is probably inadequate for collecting clear audio recordings. We have therefore focussed in this article on the use of optical surveillance devices.

In Victoria, the Northern Territory and Western Australia, surveillance legislation prohibits the installation, use and maintenance of optical surveillance devices to monitor or record private activities by a person who is not a party to those activities subject to exceptions, including where the parties to those private activities consent.

The New South Wales Act, the *Surveillance Devices Act 2007*, is narrower. It prohibits the installation, use, or maintenance involving entry onto premises, or entry into or interference with a vehicle or object, without the express or implied consent of the owner or occupier of the premises or the individual having lawful possession or control of the vehicle or object. The effect of this is that it is likely to apply in the same circumstances in which trespass issues arise.

An "optical surveillance device" is defined broadly in each Act. For example, in the NSW Act it is defined to mean "any device capable of being used to record visually or observe an activity", and is likely to include binoculars, telescopes, cameras, video cameras, security cameras, closed-circuit television (CCTV) and webcams. However, glasses, monocles, contact lenses and similar devices used by persons with impaired sight to overcome the disability are specifically excluded from the definition.

Consequently, use of a camera attached to a drone is likely to be use of an "optical surveillance device" and care needs to be taken in every case to ensure that the applicable laws are complied with.

The ACT has workplace surveillance legislation, the *Workplace Privacy Act 2011*, but does not have general surveillance prohibitions. NSW has workplace surveillance legislation, the *Workplace Surveillance Act 2010*, in addition to the general Act above.

3. PRIVACY

3.1 Regulation under the *Privacy Act 1988* (Cth)

Drones that are used to take photographs in places where there are people may collect "personal information" as defined by the *Privacy Act 1988* (Cth).

Media organisations which have publicly committed to standards which deal with privacy in a media context have the benefit of the journalism exemption to the *Privacy Act*, which applies in relation to acts in the course of journalism. That is likely to be available in respect of any use of drones in the course of gathering news.

Media organisations must of course take into account and comply with the standards to which they have publicly committed. In general terms, such standards generally require that media organisations refrain from invading a person's privacy unless there is a public interest reason to do so: see for example clause 3.5.1 of the *Commercial Television Code of Practice*; the Press Council's *Statement of General Principles* and *Statement of Privacy Principles*; clause 2.2 of the *Subscription Television Code of Practice*; and clause 2.3(d) of the *Commercial Radio Code of Practice*.

The *Privacy Act* is an important consideration for non-media organisations and for media organisations outside of the scope of journalism. Personal information is defined in the Act to include information about an identified individual, or an individual who is reasonably identifiable. This means that photographs which show people's faces are likely to be "personal information" regulated by the Act where they are collected by an entity such as a Commonwealth Government Agency to which the Act applies.

The Privacy Act does not generally affect use of drones by individuals for personal or domestic reasons. This is, among other things, because the Act contains a carve out in relation to the non-business activities of individuals under s16 for the collection of personal information for personal, family or household affairs.

The *Privacy Act* only permits collection of "sensitive information" generally where there is consent or another exception applies. An interesting question which has been discussed in Privacy circles for many years is whether or not a photograph constitutes "sensitive information" on the basis that it conveys information

about an individual's health. A pragmatic approach is taken to this issue by most entities, in that there are many circumstances (such as where a crowd is involved) in which as a matter of practice photographs are taken without people's consent, or in which it is arguable that no health information is conveyed. It can be argued that where a person is in a public place, such consent may be implicit.

In addition, Australian Privacy Principle 6 prevents use or disclosure of information for a purpose other than the primary purpose of collection.

There are also interesting questions about how Australian Privacy Principle 5, which requires that reasonable steps be taken to ensure that individuals are aware of particular specified matters, can be met where information is collected in this way. The Privacy Commissioner's Guidelines acknowledge that there are circumstances in which "reasonable steps" means taking no steps at all and it is arguable that this is such a circumstance. However, until tested and clarified, some uncertainty will remain.

3.2 Cause of action

Since the decision of the High Court in *Australian Broadcasting Corp v Lenah Game Meats* (2001) 208 CLR 199, the way has been open for introduction in Australia of a tort of a cause of action for interference with privacy. A majority of the court in *Lenah Game Meats* found that the High Court's decision in *Victoria Park Racing and Recreation Grounds Co Ltd v Taylor* (1937) 58 CLR 479 does not stand in the way of development of such a tort.

No member of the court in *Lenah Game Meats* actually held there is a privacy tort. Callinan J was the only judge who appeared to clearly favour development of the tort, stating at [335] that:

> "It seems to me that, having regard to current conditions in this country, and the developments of the law in other common law jurisdictions, the time is ripe for consideration whether a tort of invasion of privacy should be recognised in this country, or whether the legislatures should be left to determine whether provisions for a remedy for it should be made."

Gummow and Hayne JJ (with whom Gaudron J agreed) and Callinan J each discussed in detail in their judgments the possibility of a tort. Gummow and Hayne JJ found that any tort would protect individuals and not corporations. They discussed the United States tort at length and with apparent approval (stating, for example, in respect of corporate privacy, that any Australian tort "not depart from the course which has been worked out over a century in the United States": at ([129)]. However, they did not express any concluded view on whether such a tort should develop in Australia. Nor did they express any view that the approach taken in the United Kingdom of extending the law of confidentiality is correct.

Gleeson CJ in *Lenah Game Meats* found that the law of confidence in Australia should develop in the same way as in the United Kingdom. Gleeson CJ said that:

> The nature of the information must be such that it is capable of being regarded as confidential. A photographic image, illegally or improperly or surreptitiously obtained, where what is depicted is private, may constitute confidential information. In *Hellewell v Chief Constable of Derbyshire* [[1995] 1 WLR 804 at 807; [1995] 4 All ER 473 at 476, Laws J said:
>
> > If someone with a telephoto lens were to take from a distance and with no authority a picture of another engaged in some private act, his subsequent disclosure of the photograph would, in my judgment, as surely amount to a breach of confidence as if he had found or stolen a letter or diary in which the act was recounted and proceeded to publish it. In such a case, the law would protect what might reasonably be called a right of privacy, although the name accorded to the cause of action would be breach of confidence. It is, of course, elementary that, in all such cases, a defence based on public interest would be available. I agree with that proposition, although, to adapt it to the Australian context, it is necessary to add a qualification concerning the constitutional freedom of political communication.

Gleeson CJ gave some guidance as to what activities might be relevantly "private" (at [42]):

> There is no bright line which can be drawn between what is private and what is not. Use of the term "public" is often a convenient method of contrast, but there is a large area in between what is necessarily public and what is necessarily private. An activity is not private simply because it is not done in public. It does not suffice to make an act private that, because it occurs on private property, it has such measure of protection from the public gaze as the characteristics of the property, the nature of the activity, the locality, and the disposition of the property owner combine to afford. Certain kinds of information about a person, such as information relating to health, personal relationships, or finances may be easy to identify as private; as may certain kinds of activity, which a reasonable person, applying contemporary standards of morals and behaviour, would understand to be meant to be unobserved. The requirement that disclosure or observation of information or conduct would be highly offensive to a reasonable person of ordinary sensibilities is in many circumstances a useful practical test of what is private.

Gleeson CJ favoured the development of the law of confidentiality to protect privacy and only briefly considered the possibility of a tort (which it appears from his Honour's position on confidentiality he did not favour).

it is doubtful whether the test for trespass into airspace would apply to drones

Kirby J deferred the question of whether there is any cause of action for invasion of privacy altogether and did not consider whether any such cause of action would be a tort or part of the law of confidence.

The United States privacy tort is likely to be very influential in the development of any Australian tort. Judges representing a majority of the court (Gummow and Hayne JJ, with whom Gaudron J agreed, and Callinan J) discussed the United States privacy tort in some detail. The US privacy tort is divided into four categories:

1. intrusion upon seclusion;
2. appropriation of name or likeness;
3. publicity given to private life; and
4. publicity placing a person in a false light.

It is likely that any tort of invasion of privacy in Australia would be similar to the third category, "publicity given to private life", which, as noted by Gummow and Hayne JJ in *Lenah Game Meats* is described as follows:

> One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicised is of a kind that:
>
> a) would be highly offensive to a reasonable person; and
>
> b) is not of legitimate concern to the public: *Lenah Game Meats* at [120], quoting Restatement of the Law, Second, Torts.

A number of cases have been decided since *Lenah Game Meats*, but none has yet progressed to the High Court, where the existence or otherwise of privacy rights at tort will no doubt ultimately be determined.

In *Grosse v Purvis* [2003] Aust Tort Reports 81-706; [2003] QDC 151 the Queensland District Court found that a common law tort of privacy existed. An appeal against this decision was discontinued. In that case, Skoien J noted that no right to privacy existed in the common law, and saw it as a "bold" but "logical and desirable step" to be the first to find such an actionable right existed in the circumstances. Judge Skoien found that to establish the tort, it was necessary to establish the following elements:

a) [that there was] a willed act by the defendant;

b) which intrudes upon the privacy or seclusion of the plaintiff;

c) in a manner which would be considered highly offensive to a reasonable person of ordinary sensibilities; and

d) which causes the plaintiff detriment in the form of emotional or physical harm or distress which prevents or hinders the plaintiff from doing an act which she is lawfully entitled to do.

Justice Hampel found both a cause of action based on a tort of privacy and one based on breach of confidence in a 2007 case against the Australian Broadcasting Corporation involving identification in a news broadcast of a sexual assault victim in *Doe v ABC* [2007] VCC 281. In that case, the victim of sexual assault was awarded general and special damages in the sum of $234,190 after three separate ABC news bulletins identified her rapist by name, revealed that the offences had occurred in the victim's home, and named the suburb and described the area of Melbourne where the suburb is located. In addition, one of the bulletins referred to the victim by name. The ABC appealed the decision, but then agreed to have the appeal dismissed by consent. The substantive issues raised have not therefore been considered at an appellate level.

In *Seven Network (Operations) Ltd v Australian Broadcasting Corporation* [2007] NSWSC 1289, Barrett J found there was a serious question to be tried as to whether the Australian Broadcasting corporation, or entities associated with the Chaser's War on Everything, had "breached an equitable obligation of confidence of the kind recognised at various parts of the judgments in *Lenah Game Meats Pty Ltd* and in *Douglas v Hello! Ltd* [2007] UKHL 21 where the Chaser had entered the Seven premises in Martin Place to perform a "stunt" for the show. His Honour said that:

> "... confidences go to a number of matters, the peripheral aspects of which are probably the means of access to the premises, while the central aspects are matters to do with the production and content of the Channel 7 program "Today Tonight", including matters such as the layout of the production premises (described by the Chaser team on the film as "the temple of mediocrity") and the planning of the "Today Tonight" program displayed on boards on the wall of the work area."

In *Giller v Procopets* (2008) 24 VR 1; [2008] VSCA 236 the Victorian Court of Appeal found that the plaintiff was entitled to damages for distress for breach of confidence and that it was unnecessary to decide whether there is a tort of privacy.

In that case it was found that the defendant had videotaped sexual activities involving himself and the plaintiff, had shown it to be at least two people and had tried to show it to other people. The plaintiff had not consented to any disclosure of the tapes; and was found to have suffered mental distress falling short of psychiatric injury.

The court found that disclosure of the tapes constituted a breach of confidence. That finding is consistent with traditional breach of confidence principles which apply in Australia in that it was held that the videotape of sexual activities contained information imparted in circumstances giving rise to an obligation of confidence on the part of the defendant. The decision is not therefore authority in support of an extended obligation of confidence which would protect private information in the absence of such a relationship, which is the English approach supported by Gleeson CJ in *Lenah Game Meats*. However the court does appear from the judgments to have been generally supportive of the Gleeson approach. However, the court's finding that compensation can be awarded for distress falling short of psychiatric injury is a significant extension of the law of confidence which is likely to result in breach of confidence claims analogous to defamation claims (and often in tandem with defamation claims).

However, in *Kalaba v Commonwealth* [2004] FCA 763, Heerey J found that there is not yet a tort of privacy in Australia and that "the weight of authority … is against" the proposition that there is such a tort (at [6]).

Likewise, in *John Fairfax Publications Pty Ltd v Hitchcock* [2007] NSWCA 364, McColl JA stated at [124]:

> "Australian common law does not recognise a tort of privacy, although some members of the High Court have tentatively acknowledged that such a tort may emerge, at least for individuals rather than corporations."

McColl JA's statement was quoted and followed by the decision in *Maynes v Casey* (2010) 13 DCLR (NSW) 83 which is a decision of the NSW District Court which declined to recognise a tort of breach of privacy in Australia.

Thus the case law is at this stage mixed and there is no clear trend. In *Dye v Commonwealth Securities* [2010] FCA 720, Katzmann J noted the uncertain state of the law as to the existence or otherwise of a tort for breach of privacy, stating at [290]:

"I accept, therefore, that it would be inappropriate to deny someone the opportunity to sue for breach of privacy on the basis of the current state of the common law, although whether the matters complained of in the present case would be actionable if a tort of privacy were recognised is another question."

The position will no doubt eventually be clarified by the High Court. Until this occurs, it is inevitable that claims will from time to time be made, and that varying decisions will be made by the lower courts.

It is easy to imagine circumstances in which a cause of action for breach of privacy could be alleged. These include where, for example, drones are flown over suburban backyards and record private activities of residents, which could later be published online or in the media or where a moment of particular personal distress or of intimate engagement is caught on camera by a drone. Unlike the *Privacy Act*, a cause of action would not have any media exemption.

4. NO STATUTORY CAUSE OF ACTION FOR BREACH OF PRIVACY – YET

Recommendations by various law reform bodies for a statutory cause of action have so far successfully been resisted by media organisations. In August 2008, the Australian Law Reform Commission released *For Your Information: Australian Privacy Law and Practice Report* dated May 2008 (the "Report") which proposed extensive national reforms of Australian privacy laws, including a new statutory cause of action for breach of privacy and adjustments to the media exemption in the Privacy Act 1988 (Cth). In May 2007, the New South Wales Law Reform Commission released a consultation paper which also proposed a new statutory cause of action for invasion of privacy.[3]

it can be expected that the Courts will start to clarify the many uncertainties which currently exist in relation to drone use. Courts will need to balance the public interest in utilising the benefits which drone technology has to offer against the public interest in protecting privacy and other individual rights

Most recently, on 3 March 2016, the Standing Committee on Law and Justice of the NSW Legislative Council published a report entitled "Remedies for the Serious Invasion of Privacy in New South Wales" which recommended that the NSW Government introduce a statutory cause of action for serious invasions of privacy. It recommended that the cause of action be based on the Australian Law Reform Commission model detailed in the 2014 report *Serious Invasions of Privacy in the Digital Era*. It recommended that the NSW Government should also consider incorporating a fault element of intent, recklessness and negligence for governments and corporations, and a fault element of intent and recklessness for natural persons. The Standing Committee cited concerns about drones as a significant consideration, whilst acknowledging that it had not heard from anyone who had been adversely affected by use of drones.

In relation to each of these law reform proposals, media organisations have pointed out that any cause of action could have an adverse effect on freedom of communication and would add to the thicket of laws which already protects privacy interests in relation to media reporting (such as court reporting restrictions). Freedom of communication is of course im-

3 http://www.lawlink.nsw.gov.au/lawlink/lrc/ll_lrc.nsf/pages/LRC_cref113.

portant to the community as a whole, and not just to media interests: as Louis D. Brandeis (widely credited as one of the fathers of privacy law) famously said in *Other People's Money – and How Bankers Use it* in 1914:

> "Publicity is justly commended as a remedy for social and industrial diseases. Sunlight is said to be the best of disinfectants; electric light the most efficient policeman."

It is likely that any cause of action will burden freedom of communication, including freedom of communication about government and political matters. This means that it will need to pass the test enunciated by a majority of the High Court in *McCloy v New South Wales* [2015] HCA 34 in order to be valid. That test requires that the purpose of the law and the means adopted to achieve that purpose be legitimate, in the sense that they are compatible with the maintenance of the constitutionally prescribed system of representative government. It also requires that the law be reasonably appropriate and adapted to advance that legitimate object.

5. TRESPASS

There are also issues about how the laws of trespass apply in relation to drones. A cause of action for trespass to land can arise where there is intrusion into property. In *LJP Investments v Howard Chia Investments* (1989) 24 NSWLR 490, the Supreme Court found that trespass to airspace will occur where the interference is "of a nature and at a height which may interfere with any ordinary uses of the land which the occupier may see fit to undertake." This test has since been approved and applied in cases which deal with a physical encroachment, rather than an aircraft encroachment onto property, such as *Bendal Pty Ltd v Mirvac Project Pty Ltd* (1991) 23 NSWLR 464 and *Break Fast Investments Pty Ltd v PCH Melbourne Pty Ltd* (2007) 20 VR 311.

However, it is doubtful whether the test for trespass into airspace would apply to drones. Bryson J stated in *Bendal v Mirvac* at 470 that activities above the surface of land which cease to have a sufficiently close relationship with it will not be protected by the law of trespass, citing the English case of *Bernstein of Leigh (Baron) v Skyviews & General Ltd* [1978] QB 479. *Bernstein of Leigh v Skyviews* concerned an action of trespass and invasion of privacy for flying over the plaintiff's land to take an aerial photo of the plaintiff's country house that the plaintiff had offered to sell to the defendants. Griffiths J found that the defendant's flight over the plaintiff's property was not trespass because flying hundreds of feet above the ground did not cause any interference with any use to which the plaintiff might wish to use his land. Furthermore, the mere taking of a photograph could not constitute trespass into the plaintiff's airspace. However, Griffiths J suggested that activity such as constant surveillance and harassment could constitute trespass, stating at 489 that:

> "although an owner can found no action in trespass or nuisance if he relies solely upon the flight of the aircraft above his property as founding his cause of action, the section will not preclude him from bringing an action if he can point to some activity carried on by or from the aircraft that can properly be considered a trespass or nuisance, or some other tort."

The issue of trespass into airspace by an overflying aircraft has not been dealt with in Australia, and it remains to be seen whether the courts would follow the decision in *Bernstein of Leigh (Baron) v Skyviews* in relation to drones.

In considering the Australian position concerning drones used to record activities on private property, existing media cases are likely to be a key consideration. Courts recognised an implied licence to enter a property to approach the occupier to request permission to film, but in the absence of permission filming on private land may constitute a trespass. For example, in *TCN Channel Nine Pty Ltd v Anning* (2002) 54 NSWLR 333; [2002] NSWCA 82, a television news crew entered a residential property with the intention of filming a police raid on the premises and conducting interviews with a view to broadcasting. District Court Judge English found that TCN Channel Nine Pty Ltd did not have any express or implied licence to enter and remain on the property to film and had committed the tort of trespass to land. On appeal, the NSW Court of Appeal unanimously upheld English DCJ's finding. The *Anning* decision was followed in *Craftsman Homes Australia v TCN Channel Nine Pty Ltd* [2006] NSWSC 519.

By analogy a Court may well find that, where a drone is found to have entered upon private property, the permission of the occupier is required to lawfully film.

6. CONCLUSION

Where common sense is exercised it is likely that use of a drone will not upset anybody and will not result in any claims.

It is also inevitable, however, that at some stage someone will use a drone in Australia so as to seriously offend someone or to cause a substantial loss.

When that occurs, it can be expected that the Courts will start to clarify the many uncertainties which currently exist in relation to drone use. Courts will need to balance the public interest in utilising the benefits which drone technology has to offer against the public interest in protecting privacy and other individual rights.

In the meantime, it is prudent for those who wish to fly drones to carefully assess the legal risks involved in relation to each intended use.

The Types of Telecommunications Device Identification and Location Approximation Metadata: Under Australia's Warrantless Mandatory Metadata Retention and Disclosure Laws

By Stanley Shanapinda, Ph.D. Candidate, UNSW SEIT (ACCS, UNSW Law, D2D CRC)

INTRODUCTION

This article briefly discusses the legal duties of Australian telecommunications service providers (**Telcos**) to access, use, retain, create and disclose device identification and location information. In this context, the device identification and location information is the relevant metadata. The article also touches on the powers of law enforcement and national security agencies (**the Agencies**) to authorise the disclosure, access and use of the device identification and location metadata. It provides a brief description of the types of identification and location metadata Telcos are legally compelled to retain, create and disclose. The intention of this article is to describe to lawyers, who practise in the areas of communications and privacy law, six of the methods that may be used to identify and approximate the physical or logical location of fixed or mobile telecommunications devices.

COMPELLED ASSISTANCE

Telcos are required to provide such help as is reasonably necessary to the Agencies. Compelled assistance is imposed by subsections 313(3), (4) and (7) of the *Telecommunications Act 1997 (Cth)*. Reasonably necessary assistance means the disclosure of identification and location metadata of telecommunications equipment or a line used in connection with a communication. The duty to retain the metadata prior to its disclosure is set out in subsection 187A and subsection 187AA (1) of the *Telecommunications Interception and Access Act 1979 (Cth)* (**TIA Act**), in Items 2, 3 and 6 of the data set specifically. Identification and location metadata are required to be retained for a period of two years or more, in terms of section 187C of the TIA Act. In judge and jury fashion, the device identification and location metadata must be disclosed upon authorisation by the very same Agencies, without requiring a judicial warrant. Under the TIA Act, the device identification and location metadata may be historical or prospective.

METHODS FOR DEVICE IDENTIFICATION AND LOCATION APPROXIMATION

The identification and detection of the approximated location of telecommunications devices may be done in any of the six methods, briefly described below. The devices may be mobile (wireless), fixed, or fixed-wireless.

Mobile wireless devices may include Wi-Fi routers and modems; tablets; dumb phones and smartphones. Fixed devices may include fixed-line telephone devices and ADSL. Fixed-mobile devices include WiMAX and HFC cable networks, such as those offered by the NBN Co.

Other devices and equipment include the Base Transceiver Station (**BTS**) housed close to a cell tower and the physical location of the actual physical tower. Identification and location detection may be done by both or either of the parties. This may depend on whether raw location data is retained and disclosed, that may require triangulation.[1]

Using GNSS (Global Navigation Satellite System)

As the name suggests, GNSS includes all the satellite systems of the world. It includes GPS, the American system; Galileo, the EU system that is currently being deployed; and the Russian system GLONASS; but not limited thereto. There is no telling which system a device is using. Apple uses Assisted GPS and GLONASS. The location is approximated in terms of latitude, longitude and possibly altitude, and may have an accuracy of between 15m to 1m. It is never precise, and even less so in urban areas, than in an open field.[2]

1 ACMA. (2010). *Mobile location information Location assisted response alternatives*. Retrieved from Canberra http://www.acma.gov.au/webwr/_assets/main/lib311840/mobile_location_information_location_assisted_response_alternatives.pdf.

2 Forensics, C. M. (Producer). (2015, 14 May 2016). Understanding Location Information Extracted From Mobile Devices Professor David Last. Retrieved from https://www.youtube.com/watch?v=6rm4wixUPzk&feature=youtu.be&elqTrackId=6AE31B9C63C526AA355016A1D00F; and Apple. (2016). iPhone 6. Retrieved from http://www.apple.com/au/iphone-6/specs/.

3 Brandis, G. (2015). *Telecommunications (Interception And Access) Amendment (Data Retention) Bill 2015 Revised Explanatory Memorandum*. Canberra: THE PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA Retrieved from http://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r5375_ems_ac4732e1-5116-4d8f-8de5-0ead3828012c/upload_pdf/501754%20Revised%20EM.pdf;fileType=application%2Fpdf#search=%22legislation/ems/r5375_ems_ac4732e1-5116-4d8f-8de5-0ead3828012c%22; p.50.

According to the revised Explanatory Memorandum submitted with the *Telecommunications (Interception And Access) Amendment (Data Retention) Bill 2015*, the Telcos are not required to keep the continuous GPS location of a device.[3]

The intention of this article is to describe to lawyers, who practise in the areas of communications and privacy law, six of the methods that may be used to identify and approximate the physical or logical location of fixed or mobile telecommunications devices

Using the Subscriber's Address

The simplest method is using the subscriber's residential and/or business address.[4]

It is for this reason subscribers of either fixed, mobile or fixed-mobile telecommunications services are required to submit identity and residential documentation. Prepaid mobile subscribers have been legally compelled to do so since 1997. Telcos are forbidden to activate any pre-paid mobile services for which no identity documentation is submitted. No subscriber will be rendered a service and no Universal Integrated Circuit Card (**UICC**) will be activated in respect of that subscriber, unless the identification requirements have been met. These are requirements in terms of the *Telecommunications (Service Provider – Identity Checks for Prepaid Mobile Carriage Services) Determination 2013*.[5] The subscriber may be required to notify the Telco of any address changes, or if and when the UICC is lost or stolen.

Using the Telco's Network

Using the UICC

The UICC is a smart card, the IC (Integrated Card). It is commonly referred to as the SIM-card. The UICC has an Integrated Circuit Card Identifier (ICCID) that consists of the number 89, representing the telecommunications industry, the country code, and the MNC, e.g. 03 and a 14 digit code. The location area of the device is stored on the SIMs.

The smart card contains the SIM-card or the USIM-card software applications (Project, 2015). These in turn contain the IMSI (International Mobile Subscriber Identity). Without the IMSI no cellular phone service can technically be provided to the subscriber. It is used to identify and authenticate the subscriber to use the cellular network. The IMSI differentiates the subscriber from all other users of the network.[6]

The IMSI consists of three fields, i.e. the mobile country code (**MCC**), the mobile network code (**MNC**), and the mobile subscription identification number (**MSIN**) or mobile identification number (**MIN**). Australia's MCC is 505 and Telstra's network code is 01, for example. The MSIN is a 10-digit number that uniquely identifies a subscriber. It is issued by the Telco to register the subscriber, to authenticate the handset for use, to retrieve any subscription data and for billing purposes.[7]

The MSIN and the Mobile Station ISDN (MSISDN) are associated to identify the subscriber.[8]

The MSISDN comprises the CC (Country Code) and the National (significant) mobile number. The National (significant) mobile number in turn comprises the NDC (National Destination Code) and the Subscriber Number (SN).[9] Australia's CC is 61.[10]

This may be what makes IMSI-catchers or cell site simulators, branded as StingRay amongst others, popular with American agencies such as the FBI and the NSA.

Using BTS

Telcos are also required to retain and disclose the location of the BTS.[11] The device can use the Base Station Identify Code (BSIC) to differentiate between two BTSs. This is a 6 bit color code.[12]

To approximate the location of a mobile cellular device, the unique ID of the cell within the Telco's network must be determined. This unique ID is called the Cell Global Identification (**CGI**). The CGI is in turn identified from the Location Area Identification (**LAI**) and the Cell Identity (CI).[13]

4 Attorney General's Department (2015). *DATA RETENTION Frequently Asked Questions for Industry*. Canberra: Attorney General Department Retrieved from https://www.ag.gov.au/NationalSecurity/DataRetention/Documents/DataRetentionIndustryFAQS.pdf; p22.

5 *Telecommunications (Service Provider – Identity Checks for Prepaid Mobile Carriage Services) Determination 2013* (Cth), section 2.3.

6 ITU. (2011). List Of ITU-T Recommendation E.164 Assigned Country Codes ITU, p.1.

7 ITU. (2008). The international identification plan for public networks and subscriptions *SERIES E: OVERALL NETWORK OPERATION, TELEPHONE SERVICE, SERVICE OPERATION AND HUMAN FACTORS* (pp. 1). Geneva: ITU-T; p.2.

8 ETSI. (2016), Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); Numbering, addressing and identification (pp. 22, 24, 25). Sophia Antipolis Cedex - FRANCE: ETSI; pp. 16, 22.

9 Ibid.

10 ITU, (2011).

11 Brandis, G. (2015); p. 50.

12 ETSI. (2016), Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); Numbering, addressing and identification (pp. 22, 24, 25). Sophia Antipolis Cedex - FRANCE: ETSI; p. 25.

13 Ibid.

The LAI comprises the MCC, the MNC and the Location Area Code (LAC). The LAC is a hexadecimal number issued by the system.[14]

These identifiers are used to triangulate the position of the device in question.[15]

Triangulation algorithms

Triangulation algorithms are used to locate mobile devices. The two methods are the Cell ID (CID)-RTT (Round Trip Time) and the Radio Frequency (RF) pattern matching method.[16]

In the Cell ID-RTT method the distance from the corresponding cell to the device is calculated, using the Timing Advance (TA).[17] Every RTT measurement is used to calculate the distance. The intersection of the RTT circles is taken to be the location of the device. With the RF pattern matching method, in addition to using the CellID RTT method, a comparison of the radio signal strengths is used.[18]

However, Telcos are not required to conduct additional processing or triangulation. Telcos can simply provide the RTT measurements and the database of the signal strengths, if available from the network.[19]

Using the Handset

Whereas the IMSI is used to identify the user, the International Mobile Station Equipment Identity (**IMEI**) is used to identify the mobile handset. The IMEI contains the origin, model and serial number of the handset.[20]

The IMEI can be retrieved by typing the Unstructured Supplementary Service Data (USSD) code *#06# into the keypad of most mobile phones.

Using the WLAN (Wireless Local Area Network)

Each mobile device has a Media Access Control (**MAC**) address assigned to it by the manufacturer. The MAC address is required to be stored and disclosed.[21] This number was generally static but may be dynamically assigned, by the likes of Apple. MAC addresses are used for billing purposes to uniquely identify the subscriber. It consists of six groups of two hexadecimal digits, with six octets.[22]

When a Wi-Fi router or smart phone detects a WLAN, it will determine if the MAC address is white-listed to use its services. If it is, it will be authenticated, after the correct password is entered and accepted, if required. The MAC address is filtered in this manner.[23] The MAC address is defined as a telecommunications number in section 5 of the TIA Act and must be retained and disclosed, under that legislation.

Using the Hybrid Method

Telcos and the Agencies may generally use a combination of the above methods. These include cell tower signal strength, wireless signal strengths for internet connectivity, Bluetooth sensors and IP addresses.

CONCLUSION

As one can readily see, there are many methods by which a telecommunications device, whether fixed or mobile, can be identified. Through those processes, it is also possible to identify the person registered to operate that device (although not necessarily the person using the device at any particular time), in relation to a criminal investigation, a cybercrime investigation or intelligence gathering for national security purposes. The types of location information and the approximation methods described are by no means a closed list of location metadata.

No doubt, the techniques used to locate and identify end users will evolve as the technology does

No doubt, the techniques used to locate and identify end users will evolve as the technology does. Lawyers advising telecommunications companies and their customers, or security or law enforcement agencies, will need to familiarise themselves with some of the internal architecture of the telecommunications devices that have become a defining feature of the modern digital economy.

14 Ibid., p. 24.

15 ACMA. (2010); p.7.

16 ETSI. (2010). Universal Mobile Telecommunications System (UMTS); Evaluation of the inclusion of path loss based location technology in the UTRAN (3GPP TR 25.907 version 9.0.1 Release 9) p.14; Clarke, R., & Wigan, M. (2011). You are where you've been: the privacy implications of location and tracking technologies. *Journal of Location Based Services, 5*(3-4), 138–155. doi:10.1080/17489725.2011.637969; p,144; ACMA (2010), pp. 7, 9, 14.

17 ETSI. (2016). Digital cellular telecommunications systems (Phase 2+) (GSM) Functional stage 2 description of Location Services (LCS) in GERAN (3GPP TS 43.059 version 13.1.0 Release 13) (pp. 8,10, 11,12,13,14). Sophia Antipolis Cedex – FRANCE; p.12.

18 ETSI (2010), p. 14.

19 Attorney General's Department, p. 15.

20 ETSI. (2009). 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; International Mobile station Equipment Identities (IMEI) (Release 9) (pp. 5). Sophia Antipolis Valbonne - FRANCE: ETSI; p.5.

21 Attorney General's Department, p. 14.

22 IEEE. (2016). Guidelines for 64-bit Global Identifier (EUI-64). Retrieved from https://standards.ieee.org/develop/regauth/tut/eui64.pdf.

23 Huawei Technologies Co, L. (2012). WLAN Access Security Technical White Paper(2), 3. Retrieved from http://e.huawei.com/en website: http://e.huawei.com/uk/marketing-material/onLineView?MaterialID=%7BA944F23F-EF58-43E5-AF55-AC7951B73E83%7D.

The Complex Web: The Global Network, Snowden, Safe Harbours, Shields and the GDPR

Daniel Cater; BNSc (Dis), Juris Doctor (Hon), Phd student UNSW

INTRODUCTION

Data production is inherent in the internet. Myriad devices constantly produce huge volumes of data as part of everyday living in the information age and this data moves and is stored in servers and 'clouds' regardless of territorial borders. Logging onto a device and connecting to the internet produces data as both input and output, it can include everything from transaction and communication records to timestamps and location and it may be intentional or coincidental.[1] In the digital environment data moves rapidly and unpredictably, it can move in segments and be stored in multiple locales, it can be conglomerated with unrelated data, and data locality can be completely separate from involved parties.[2] Data often travels beyond either the control or knowledge of concerned parties, who have little or no influence over it, and it can be remotely accessed from sites hugely distant of its physical location.[3] The production of data has become an unavoidable aspect of integration into the modern world; this data is generated in massive volumes and can be moved, stored and accessed anywhere on the planet.

The production of data has become an unavoidable aspect of integration into the modern world; this data is generated in massive volumes and can be moved, stored and accessed anywhere on the planet

The rapid transfer and storage of data is essential to global communication and economies but it also presents threats to the security of that data as well as privacy; benefits and risks which increase as networking technology develops. Governments and international bodies have all recognised the critical role which rapid and efficient international data flow plays in economies, international development and global stability as well as the potential security and privacy threat it represents.[4] In Australia, Europe and across North America individuals, organisations and governments are all critical users of the global internet and must address its benefits and risks.

THE SNOWDEN EFFECT AND SCHREMS

In 2013 Edward Snowden, a US intelligence contractor, leaked documents revealing massive government surveillance programs with international reach; disclosures which caused worldwide anger and condemnation. The Snowden revelations related to widespread mass surveillance by the US and its allies, in particular its 'Five Eyes' treaty partners[5], provoked public debate and outraged privacy advocates.[6] Recent studies have indicated the Snowden leaks have reduced trust in data integrity and privacy online and resulted in reductions in both economic activity and internet free speech.[7] The Snowden leaks have thus become a watershed in changing social perception of government surveillance and formed a rallying point in demands for greater transparency and privacy protections online.[8] Individuals across the world now have height-

1 Schneier, Bruce, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (W. W. Norton & Company, 2015), p15-20.

2 Daskal, Jennifer, 'The Un-Territoriality of Data' (November 2015) 125(2) *The Yale Law Journal* 326, p366-78.

3 Ibid p333, 357, 369-74.

4 Office of the United Nations High Commissioner for Human Rights, 'The Right to Privacy in the Digital Age' UN Doc A/HRC/27/37 (30 June 2014); Organisation for Economic Co-operation and Development [OECD], *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (11 July 2013) http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf; The Executive Office of the President 'Big Data: Seizing Opportunities, Preserving Values' (Review, The White House, May 2014); Department of Foreign Affairs and Trade, *FTA Chapter Summaries*, Trans-Pacific Partnership Chapter Summary: Electronic Commerce (12 November 2015) http://dfat.gov.au/trade/agreements/tpp/summaries/Documents/electronic-commerce.PDF

5 The Five Eyes group are the nations of Australia, Canada, New Zealand, the United Kingdom and the United States of America which have a series of bilateral intelligence and communication sharing agreements with their origin in the 1946 UKUSA Agreement; http://www.asd.gov.au/partners/allies.htm & https://www.nsa.gov/public_info/declass/ukusa.shtml.

6 Milanovic, Marko, 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age' (Winter 2015) 56(1) *Harvard International Law Journal* 81, p81-2.

7 Goldberg, Rafi, 'Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities' (13 May 2016) *National Telecommunications & Information Administration Blog* https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities; Penney, Jonathon W., 'Chilling Effects: Online Surveillance and Wikipedia Use' (May 2016) *Social Science Research Network* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2769645

8 Raab, Charles D., Richard Jones and Ivan Szekely, 'Surveillance and Resilience in Theory and Practice' (2015) 3(2) *Media and Communications* 21, p34-5.

ened awareness of the reach which bulk data surveillance operations have and are demanding action from the governments and corporations.

One major impact of this increased disquiet over transborder data surveillance and privacy protection has been in the *Schrems Case*[9] decision in 2015 which saw the European Court of Justice (**ECJ**) overturn the US/EU *Euro Safe Harbor*[10] provisions. Mr Schrems, an Austrian, challenged Facebook's European division arguing that data transferred to Facebook's main US servers did not receive the privacy protections required in the *European Human Rights Charter* (**ECHR**).[11] The ECJ decision centred on the *Euro Safe Harbor* ruling which determined the US met the threshold which allowed data transfers outside European borders to nations which adequately protected EU citizens' rights.[12] The ECJ acknowledged that privacy is not an absolute right and must give way to the proportional needs of national security and also stated that exponential technology growth has increased the vulnerability and concerns surrounding transborder data protection.[13] The ECJ then delivered a landmark ruling holding that, given the different protection afforded US and non-US residents, the US national security data surveillance policies were not proportionate to needs and failed to provide EU citizens with basic remedies and protections.[14] The ECJ decision highlights the critical, controversial and complicated nature of privacy rights, transborder data flow, surveillance powers and jurisdiction in the information age.

While the US has been forced to address its broad domestic surveillance powers many of the provisions related to collection of foreign data remain intact. Domestically the most notable reform was the curtailing of the controversial surveillance powers enshrined in the post 9/11 *USA Patriot Act*[15] with the passing of the *USA Freedom Act*[16] in 2015. Despite these reforms the *Patriot Act's* foreign surveillance reach remained largely intact.[17] Several other provisions permitting aggressive foreign data surveillance programs also remain in place, most notably *FISA* Section 702[18] and *EO12333*[19], both legislative tools which have been foundational in US extraterritorial bulk data collection operations.[20]

The international backlash demonstrated by the ECJ *Schrems Case* decision has begun to be felt in US policy with proposed laws to limit foreign surveillance, support transparency or provide redress options. One particular example, the recently passed *Judicial Redress Act*[21], provides non-US citizens with limited redress for privacy breaches in US law, an act which directly addresses one objection in the ECJ decision; that EU citizens do not have redress rights under US law.[22] Within the US administration other figures have recognised the international ramifications of the current US foreign data policies and have proposed fur-

9 *Maximillian Schrems v Data Protection Commissioner, joined party: Digital Rights Ireland Ltd* (C-362/14) [2015] Court of Justice of the European Union.

10 *European Parliament Council Directive 95/46/EC of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data* [1995] *OJ L 281/31* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

11 O'Brien, Danny, 'No Safe Harbor: How NSA Spying Undermined U.S. Tech and Europeans' Privacy' (5 October 2015) *Electronic Frontier Foundation* https://www.eff.org/deeplinks/2015/10/europes-court-justice-nsa-surveilance and Fioretti, Julia, 'EU-U.S. data-sharing deal faces major challenge in EU court' (21 September 2015) *Reuters, Technology online* http://www.reuters.com/article/2015/09/21/us-ireland-eu-privacy-idUSKCN0RL15K201509211.

12 *Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and the Council on the adequacy of the protection provided by the safe harbor privacy principles and related frequently asked questions issued by the US Department of Commerce* [2000] OJ L 215 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML.

13 *Maximillian Schrems v Data Protection Commissioner, joined party: Digital Rights Ireland Ltd* (C-362/14) [2015] Court of Justice of the European Union, para 10, 12-3.

14 Ibid para 22, 31, 90, 93, 95.

15 *The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001*.

16 *The Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring (USA FREEDOM) Act of 2015*.

17 Froomkin, Dan, 'USA Freedom Act: Small Step for Post-Snowden Reform, Giant Leap for Congress' (3rd June 2015) *The Intercept_Unofficial_Sources* https://theintercept.com/2015/06/02/one-small-step-toward-post-snowden-surveillance-reform-one-giant-step-congress/

18 *The Foreign Intelligence Surveillance Act of 1978* and *The Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008*.

19 *Executive Order 12333 of Dec. 4, 1981, appear at 46 FR 59941, 3 CFR, 1981 Comp, p. 200* http://www.archives.gov/federal-register/codification/executive-order/12333.html

20 Buchsbaum, Emma, 'Section 702:Programmatic Collection and the Wall Reprised' (26 April 2016) *Lawfare, Surveillance, Online* https://www.lawfareblog.com/section-702-programmatic-collection-and-wall-reprised and White, Nathan, 'We Need to Know More About When the FBI Can Access One of the NSA's Biggest Databases' (29 March 2016) *Just Security Online* https://www.justsecurity.org/30300/rules-fbi-access-12333/.

21 *The Judicial Redress Act of 2015*

22 Sensenbrenner, Rep Jim, 'The Judicial Redress Act is essential to U.S. law enforcement' (17 September 2015) *The Hill online* http://thehill.com/blogs/congress-blog/homeland-security/253874-the-judicial-redress-act-is-essential-to-us-law.

23 Trujillo, Mario, 'House members push bill limiting gov access to emails stored overseas' (27 February 2015) *The Hill online* http://thehill.com/policy/technology/234121-house-members-drop-bill-limiting-gov-access-to-overseas-email and Koh, Harold Hongju, 'Memorandum Opinion on the Geographic Scope of the International Covenant on Civil and Political Rights' (19 October 2010) United States Department of State Office of the Legal Advisor found at https://www.justsecurity.org/wp-content/uploads/2014/03/state-department-iccpr-memo.pdf, p55-6.

ther reforms.[23] Nevertheless while the US government has curtailed some of the laws permitting bulk data surveillance these reforms largely focus on the domestic provisions, with slower progress on reform of powers concerning foreign data surveillance.

Understanding the political and social consequences of the Snowden leaks and the subsequent US–EU legal arguments and legislative changes, such as the GDPR, is essential in this complex area

The importance of transnational data flows has been recognised by EU and US power brokers as critical and an EU/US compromise agreement, known as the *EU-US Privacy Shield* has been negotiated, but despite these efforts EU authorities remain sceptical. One influential EU privacy advocate stated that "No one wants data transfers to stop…" but that "…information on European citizens…" cannot "… be completely without protection when they [it] leave[s] Europe".[24] The current draft of the *EU-US Privacy Shield* has been reviewed by European privacy and legal experts and its status is uncertain with the nominated Article 29 review party highlighting important concerns.[25] These apprehensions have been mirrored by the European Data Protection Supervisor who stated that the *EU-US Privacy Shield* is not robust enough to endure the inevitable legal challenges, in particular given impending EU data protection reform.[26] It remains an open question whether and when any long-term agreement on data traffic between the EU and US will be found satisfactory but the newly finalised *European General Data Protection Regulation*[27] (*GDPR*) will certainly impact the process.

THE EUROPEAN GENERAL DATA PROTECTION REGULATION

The European Union has reviewed its regional data protection and privacy regulations and passed an updated regulation which will commence legal force in 2018. The *GDPR* has been passed and will enter into force across EU states from May 2018; it is envisaged to both increase EU citizen data protection and to encourage an integrated digital economy.[28] The *GDPR* includes provisions which shield EU citizens' data globally and assert responsibilities to companies beyond Europe's borders in the management and 3rd party sharing of EU data resources.[29] The nature of these rules and the size of the EU population and economy mean that any US based or other international company wanting to access the European market will have to comply with the rules dictated in the *GDPR*.[30] The nature of the global network structure which has been established between Australia, Europe, North America and many other world economies is such that the *GDPR* will need to be considered in legal and political policy in all these jurisdictions.

The structure of the *GDPR* explicitly allows for data transfer agreements within the protective framework of the *ECHR* and further it preserves those agreements in place prior to its entry into force. The *GDPR* includes provisions for establishing international cooperation and safeguards, it preserves such agreements which existed and complied with EU law prior to its passing and it provides for extensive review and oversight.[31] The Article 29 review committee into the *EU-US Privacy Shield* released a statement that the status of any revised agreement must be further reviewed in 2018 following the *GDPR* entry into full legal force.[32] It is clear that any EU-US data sharing agreement will be required to meet the standards of the *GDPR* as it enters into effect and it will also impact other nations' interactions with data policies.

24 Fioretti, Julia, 'Europe's top privacy watchdog calls on firms to curb U.S. data transfers' (23 October 2015) *Reuters, Technology online* http://www.reuters.com/article/2015/10/23/us-europe-dataprotection-idUSKCN0SH1ZT20151023.

25 Gibbs, Samuel and agencies, 'Data regulators reject the EU-US Privacy Shield safe harbor deal, (14 April 2016) *The Guardian Technology online* https://www.theguardian.com/technology/2016/apr/14/data-regulators-reject-eu-us-privacy-shield-safe-harbour-deal. Full text of the EU-US Privacy Shield provisions is available here European Commission unveils EU-U.S. Privacy Shield (29 February 2016) *European Commission, Justice, Newsroom, Data Protection, News* http://ec.europa.eu/justice/newsroom/data-protection/news/160229_en.htm. Full text on the opinion is here *Article 29 Data Protection Working Party, 'Opinion 01/2016 on the EU–U.S. Privacy Shield draft adequacy decision'* [13 April 2016] 16/EN WP238 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf.

26 European Data Protection Supervisor, 'Privacy Shield: more robust and sustainable solution needed' (30 May 2016) *European Data Protection Supervisor, Press release,* https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2016/EDPS-2016-11-PrivacyShield_EN.pdf

27 *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)* [2016] OJ L 119/1 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

28 The European Commission, 'Protection of Personal Data', (10 May 2016) Media Release *European Commission, Justice, Data Protection* http://ec.europa.eu/justice/data-protection/

29 Above n27, Art 3, 4, 44, 45, 46.

30 Gibbs, Samuel, 'European parliament approves tougher data privacy rules' (14 April 2016) *The Guardian, Tech, online* https://www.theguardian.com/technology/2016/apr/14/european-parliament-approve-tougher-data-privacy-rules

31 Above n27, Art 46, 47, 48, 49, 50, 51, 52, 54, 96.

32 Statement of the Article 29 Working Party on the Opinion on the EU- US Privacy Shield (13 April 2016) http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/press_release_shield_en.pdf

AUSTRALIA, EUROPE AND THE GDPR

Australia is an important member of the 'Five Eyes' intelligence sharing alliance and was thus involved in the surveillance operations that were exposed by Snowden. Further, involvement in the global digital economy is critical to Australian interests. Australia is the largest 'Five Eyes' member in the southern hemisphere, and has been identified in media reports concerning both data collection and sharing with partner states, in particular the United States.[33] The draft Trans-Pacific Partnership (**TPP**) trade agreement involves a dozen countries including Australia and the US and is under review following negotiations; the agreement includes extensive data sharing provisions.[34] In TPP negotiations, Australia additionally included a Memorandum of Understanding with the US that any law extending privacy protections to foreign and non-US residents in certain countries will also provide coverage to Australian citizens.[35] While the TPP itself, like the *EU-US Privacy Shield*, remains an agreement under review, its content, and that of supporting documents, is indicative of the importance and complexity of transborder data protection.

Geographic isolation and localised laws and rights protections are increasingly irrelevant in a world where communication, business, entertainment, crime and every other facet of day-to-day life can occur online as part of the global network. The understanding and control of how data moves across borders and its value and vulnerability as a resource in business, security and privacy spheres is critical to successfully navigating benefits and risks going forward. Understanding the political and social consequences of the Snowden leaks and the subsequent US-EU legal arguments and legislative changes, such as the GDPR, is essential in this complex area.

33 Tim Leslie and Mark Corcoran, 'Explained: Australia's involvement with the NSA, the US spy agency at the heart of the global scandal' (19 November 2013) *ABC News Australia online* http://www.abc.net.au/news/2013-11-08/australian-nsa-involvement-explained/5079786

34 Trans-Pacific Partnership Agreement, 'Outcomes: Trade in the digital age' *Australian Department of Foreign Affairs* http://dfat.gov.au/trade/agreements/tpp/outcomes-documents/Pages/outcomes-trade-in-the-digital-age.aspx

35 Robb, The Hon. Andrew AO MP and Ambassador Michael B. G. Froman, 'Letter outlining Memorandum of Understanding Extending US foreign national privacy protections to Australians with regards to TPP Agreement' http://dfat.gov.au/trade/agreements/tpp/official-documents/Documents/australia-united-states-privacy-protection.PDF

Blockchain and Smart Contracts: The dawn of the Internet of Finance?

By Henry Davis York partner Matthew McMillan and lawyer Ken Wong

The 'blockchain phenomenon' opens up a myriad of opportunities for the financial services industry (including the evolution of smart contracts) but alongside the enormous potential a number of key legal considerations are emerging.

What makes blockchain truly disruptive, however, is not just the distributed nature of the ledger system but the ability to combine that with capabilities which go well beyond the traditional paper-based ledger. In particular, the ability to implement business rules into the blockchain or to enable smart contracts

Much has been spoken about of the 'trust asset' in recent times by participants in the financial services industry - in particular, the need to preserve and enhance customer trust in an organisation's brand to defend against displacement by digital disrupters.

This 'trust asset' is critical for trade to occur. It is the reason that third party banking institutions are often entrusted to facilitate payments and approve transactions.

But what if trust was enabled by technology itself, rather than an organisation's reputation or brand?

Blockchain aims to do just this. It facilitates transactions of value where trust is critical. And it does this by enabling transactions of value to occur over computer networks that can be verified, monitored and enforced without the need for trusted intermediaries.

WHAT IS BLOCKCHAIN?

Blockchain is the technology underlying bitcoin, which is a self-regulated cryptocurrency network operating without a central bank.

Blockchain operates as a distributed ledger system - essentially an asset database that can be shared across a network of multiple users in any location. Each user owns a full copy of the ledger, and plays an important role in automatically and continuously agreeing on the current state of the ledger and all of the transactions recorded in it.

The ledger is maintained through the use of cryptographic 'keys' which control who can do what, within the ledger. It is the data transparency between all users in the network, and underlying cryptography, that removes the need for a trusted intermediary.

Some of the key features of blockchain include:

- **Security and reliability:** The blockchain is a cryptographic technology that is highly resilient to attack. To attack the blockchain, an attacker would need to simultaneously compromise each user's copy of the distributed ledger. An attack on one copy (or network node) does not impact upon the availability and reliability of the information on the distributed ledger.
- **Single source of truth:** All transactions on the blockchain are visible to all users within the network, and each user plays a role in authenticating transactions on the distributed ledger, thereby removing the need for trusted intermediaries. This transparency renders it near impossible for changes to go undetected, and enhances trust and confidence in the information stored on the ledger.
- **Digital:** The blockchain allows for any asset - be it financial, legal, physical or electronic - to be expressed in code and recorded on the ledger. And because the blockchain is programmable, it can facilitate an enormous range of transactions involving those digital assets - many of which are only now being conceived.

These features open up huge opportunities for the financial services industry. This includes the ability to disintermediate trusted third parties from a wide array of transaction types. In the case of the bitcoin cryptocurrency, it is the removal of a central bank.

Rather ironically, however, it is the traditional participants in the financial services industry – the very ones which the bitcoin currency is designed to circumvent – that are increasingly investing in the underlying blockchain technology and converting what was once perceived as a threat into new opportunities to re-engineer back-end systems, increase settlement speeds and drastically drive down costs.

According to a 2015 report - by Spanish bank, Santander, management consultancy, Oliver Wyman, and venture capital investor, Anthemis - blockchain technology could cut banks' infrastructure costs for cross-border payments, securities trading and regulatory compliance by US$15bn-US$20bn a year from 2020.

BLOCKCHAIN TYPES

Broadly, there are two types of distributed ledger systems:

- **Permissionless systems**: such as the one on which bitcoin is based, where the blockchain is open to the public and the digital ledger is shared, transparent and operated by all of the users in the network.
- **Permissioned systems:** where the blockchain is controlled and administered by one or more entities and direct access to the network is limited to pre-defined users with known identities. There may be multiple layers of access to the permissioned blockchain including, for example, reading transactions, proposing new transactions and creating new blocks of transactions and adding them to the blockchain.

It is the latter which are increasingly gaining traction within the financial services industry. This is partly because of the anonymous nature of users in permissionless systems and the volatility and illicit activity that has plagued the bitcoin system.

Permissioned systems, on the other hand, more closely resemble today's financial systems and, for that reason, can more easily integrate into the mainstream economy and existing regulatory frameworks.

INVESTMENT LEVELS ARE UP

The level of investment being directed into blockchain technology by financial services organisations cannot be underestimated.

Recent examples include:

- The formation of the R3 consortium of 42 global banks to define protocols and build a platform to standardise the use of blockchain technology across relevant parts of the banking industry;
- Commonwealth Bank of Australia partnering with Ripple to facilitate blockchain-enabled payments between subsidiaries;
- Westpac's venture capital fund, Reinventure Group's, investment into Coinbase;
- Citigroup's creation of a new digital currency known as Citicoin;
- UBS' investigations into blockchain-enabled bond trading and the creation of its own digital currency in collaboration with the start-up community; and
- The ASX partnering within Digital Asset Holding to build a blockchain to run in parallel to - and, perhaps, even replace - the existing CHESS system.

BEYOND BLOCKCHAIN: THE EVOLUTION OF SMART CONTRACTS

What makes blockchain truly disruptive, however, is not just the distributed nature of the ledger system but the ability to combine that with capabilities which go well beyond the traditional paper-based ledger. In particular, the ability to implement business rules into the blockchain or to enable smart contracts.

It is at this application level (i.e. applications on top of the blockchain) that the real potential of the technology lies.

Smart contracts are self-executing contracts which are written in computer code and programmed into the blockchain. They are essentially computer protocols that facilitate, verify, execute and enforce the terms of a contract. This removes the need for human intervention as far as monitoring compliance and enforcement of the contract are concerned.

A smart contract could, for example, have code written to only allow a transaction (such as a trade) to execute at a certain time or upon the fulfilment of certain conditions. Or code which automatically deactivates the digital keys of a leased car, and prevents the car from being operated, upon a lease payment being missed. Or it could even be a set of programmed computer protocols which automate the execution of steps required to effect a real estate property settlement and enable the transfer of title.

The self-monitoring and self-enforcing nature of smart contracts has huge appeal in that it enables two parties to contract at arms' length, without the usual counterparty risk and without incurring the costs of administering and enforcing the contract.

LEGAL CONSIDERATIONS

Whilst the potential uses, benefits and risks of smart contracts are only starting to be emerge, they do give rise to some interesting and challenging legal issues. These include:

- **Formation of contracts.** To be an enforceable contract at law, the elements of contract formation will still need to be satisfied; that is, there needs to be an offer, acceptance of the offer, consideration and an intention to enter into the contract. This is not to say, however, that a smart contract is not capable of being a contract at law.
- **Interpretation and uncertainty.** Smart contracts are written in computer code, readable only by a computer system. How do the parties to the contract, a judge or a regulator interpret the terms of the smart contract?
- **Bugs and errors.** Computer code, by its nature, will often contain some form of defect. What are the potential consequences on the rights and obligations of the parties if there is a defect in the code which causes an error in the execution of the contract?
- **Ability to unwind contracts.** How does the self-executing nature of smart contracts sit with a party's rights at common law to void a contract under legal doctrines such as mistake or unconscionable conduct? Can a transaction on the block-

chain be unwound? How would this be achieved? And what would be the downstream impact for other transactions on the blockchain?

- **Confidentiality and security.** Distributed ledger systems, and smart contracts, result in massive repositories of data. To what extent is this information capable of unauthorised access or interception? Whilst cryptographic code may be difficult to break, it may nevertheless be bypassed - either through the inadvertent disclosure of cryptographic keys or 'back doors' in the software code.
- **Privacy.** An essential feature of distributed ledger systems is the public nature of the data and the ability for transactions, including smart contracts, to be publicly viewable in the ledger. This raises privacy concerns, particularly where transactions involving individuals are able to be tracked and analysed.
- **Systemic risk.** If each copy of the ledger is simultaneously attacked, or there is a distributed denial of service attack brought about by the network being overwhelmed with service requests, this could have dire consequences for the financial service industry at large. Whilst centralised ledger systems can act as shock absorbers, decentralised ledger systems cannot.
- **Jurisdiction.** Smart contracts operating in a distributed ledger system consist of a network of users from various locations. They are not specific to any one location. In the absence of an express stipulation of the governing jurisdiction in the smart contract, which jurisdiction would govern the smart contract?
- **Adjudication.** The self-executing nature of smart contracts may remove the need for legal enforcement actions. However, they don't necessarily remove the need for adjudication on other issues, such as liability arising from the execution of the contract or the need to resolve disputes.
- **Evidentiary matters.** As smart contracts will be subject to examination, there will be a need for new types of cryptography experts and forensics experts to verify software code and to translate the code into human-readable form.
- **Regulatory settings.** Smart contracts are enabling financial services to be provided in ways which disintermediate banks and other trusted intermediaries. This may not sit easily with existing regulatory and policy settings, which will need to be considered in greater detail as the technology and its applications evolve. How are regulators to police smart contracts? And what opportunities exist for parties to use blockchain-enabled smart contracts to potentially side-step the law by hiding the identity of the parties and the governing jurisdiction of the contract? How are cross-jurisdictional issues of taxation, national security and anti-money laundering to be managed?
- **Regulatory compliance.** On the flip side, smart contracts enabled by blockchain can be used to enhance transparency and auditability and facilitate better regulatory compliance. A market exchange, for example, could write rules into a smart contract requiring the rules to be met before the contract can be executed by market participants. For regulators, regulatory goals could be achieved through a mix of both laws and technical code.
- **Governance.** The nature of permissioned distributed ledger systems, and the use of smart contracts, means that there is still a need for rules and structures to be put in place for network users to adhere to. This can be challenging in a distributed network environment.
- **Decentralised organisations**. More complex smart contracts may lead to the creation of decentralised organisations, where rights are distributed and managed by the blockchain itself and ultimate responsibility may be difficult to pinpoint. Where does accountability lie? Is it the users of the distributed ledger system, the code creators or the system itself? And to what extent can existing corporations law concepts and frameworks be applied to decentralised organisations?

These issues warrant further detailed consideration as blockchain technology and the use of smart contracts evolve.

Care must also be taken to ensure that any future regulation of the technology maintains the integrity and security of the financial system without compromising the very real potential of the technology to transform the industry. This requires regulators to have a rich understanding of the technology itself, to tread softly and to exercise restraint so as not to stifle the opportunities it presents.

Profile: Sally McCausland

Owner of McCausland Law and Senior Fellow in the University of Melbourne law masters

Leah Jessup of the CAMLA Young Lawyer's Committee interviews Sally McCausland

Where do you work and can you tell us a little bit about your role?

Last year I started McCausland Media Law which is an entertainment and arts law practice. My legal work is across a range of clients in production, broadcasting and digital, theatre, arts and education, and I also do some copyright and other policy advice. When I set it up I decided that my work would be completely mobile and digital. I'm flexible with where I work and how. In my previous role as Corporate Counsel at SBS I was often going to client meetings, emailing or taking after hours calls. I realised that I didn't really need an office in the traditional sense. I don't really need to print anything. It's environmentally better and more efficient. It also means I can do occasional locum work quite seamlessly, as I've done recently at the ABC.

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

I have always been interested in the arts, in intellectual property and in journalism. While at a big law firm I got to work in IP and media. I then did a secondment at Seven Network and decided after that that I wanted to be in-house working directly with clients.

After that I went to the Arts Law Centre as supervising solicitor. It was a good way of learning more about our creative industries and how to find practical solutions for people with limited resources.

Then I went in-house at SBS. When I joined SBS it was just Lesley Power (General Counsel) and me. Lesley is a brilliant media lawyer and incredibly generous and friendly too. When I started, the SBS website was pretty basic and the online team worked in a dungeon. But over the years the digital side of the business grew and so did the legal team. During my years at SBS I got to work across many areas such as content compliance, sports contracting and fair dealing advice, policy submissions, commercial contracts, corporate governance and social media training. It taught me to be versatile and practical dealing with whatever queries came in every day from any level or area of the business.

Your previous roles have been very varied – pro bono, public broadcasting, corporate firm, judge's associate, lecturer and policy adviser. What advantages have your experiences across all of those roles given you and would you recommend that young lawyers be open to taking up a variety of roles and experiencing different aspects of the profession as you have?

Certainly I would encourage young lawyers to experience and enjoy different things. Having various roles has allowed me to get an idea about what I want out of work and keep developing new skills, rather than being pigeon-holed.

Trying different things can also lead to new opportunities. For example, in-house roles can be great as pathways to non-legal management or policy roles and you'll find that your legal skills will be really useful in those other roles.

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

A career highlight I have to mention was when I was a junior lawyer and my firm was appointed as advisers to sellers of pirated t-shirts at a Rolling Stones concert. I, along with some other juniors, had the job of standing outside the concert, approaching sellers, informing them that they were going to be served and offering them legal advice. I have a distinct memory of running across a busy road after a man who'd been selling t-shirts and who was loudly and angrily rejecting my offers of help. That was fun and what was even more fun was that we had access inside the

concert. I almost touched Mick and got my ribs slightly crushed in the process. Many years later I've had to explain to my physio why my rib cartilage is a little damaged. But it was worth it. Other career highlights have included working on the FIFA World Cup and Eurovision for SBS and doing artist workshops in the Tiwi Islands for the Arts Law Centre.

I'm always interested in what my clients are doing and the different worlds they come from. I love being close to the creative process. I think that journalists are really brave in what they do and that their work is important. And I love working with sport people because they are the happiest clients – they know they are living the dream.

My biggest challenge is time management. Ultimately my job is flexible. Sometimes if it's a beautiful day outside my husband and I will go off for a quick swim in the middle of the day. At SBS I got used to managing many different clients every day and so I'm now used to doing many things at once.

You have completed a Masters, in which you explored the legal protection of Indigenous art. How did you find juggling study and work and would you recommend that young lawyers consider pursuing a Masters?

I travelled to Canada to study my Masters after a few years working and became a student again in a share house. I had great fun going skiing on weekends and learning about bear safety while camping. My Masters looked at the laws involved in protecting communal Indigenous artworks from unauthorised exploitation. I also took subjects such as free speech regulation under the Canadian Constitution which has informed my view that Australia needs a bill of rights.

If you can afford to study and want a new focus or a break a Masters can be fabulous especially if you get to live somewhere different. I was lucky to get a fellowship which covered expenses. Studying was great fun but it is also a lot of work so you need a reason for doing it. I was really glad that I did it as my Masters led me to a job working with Indigenous artists at the Arts Law Centre when I returned to Australia. My Masters gave me an interesting perspective and led to things that I would not otherwise have done.

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

I think a big issue facing the art and entertainment industry is the digital copyright balance. The Productivity Commission and the Australian Law Reform Commission have suggested US style fair use should be introduced and this is causing a lot of concern for creators. We have small and vulnerable creative industries that really depend on copyright income. However, there are others who want more flexible use of copyright material for innovation as they see happening in the States. So there is a tension which government is being asked to resolve.

Another pressing issue is the need to develop fit for purpose defamation laws for social media. Today every person is a publisher and every business and publisher has to be on Twitter and Facebook. Yet the defamation laws are still Dickensian and badly adapted to current conditions.

Social media is also causing privacy concerns and I think it's inevitable that privacy law will evolve. But the model needs to be adaptable to solve a range of different problems and there needs to be a balance when free speech issues are in play.

What are some tips for young lawyers looking to work in this area of law?

I'd recommend that young lawyers expose themselves to a broad range of experiences early on so that they can see what they like. I'd also encourage young lawyers to think about how the profession may change in the future. Work is becoming more flexible and using only a laptop and mobile I can work flexibly with clients and around my life. The profession and courts are moving in that direction and becoming more digital. The days of commuting to an office full of paper next to the photocopier and fax machine are ending.

Young lawyers should also find themselves a good mentor. I have actively researched and sought them out during my career. Seek out the respected leaders in your field and don't be afraid to approach them. You can learn so much from just being around someone who you admire and makes you happy to be around.

LEAH JESSUP is a Senior Associate at Ashurst and member of the CAMLA Young Lawyer's Committee.

Peek at You: Pokémon GO and Capturing Player Data

By Harry Knight, Solicitor at Banki Haddock Fiora

TAKEAWAY POINTS

- mobile game developers should "obtain meaningful consent despite the small screen challenge" in accordance with the Office of the Australian Information Commissioner (OAIC) guidelines.
- personal data should only be collected if reasonably necessary for the mobile game to function, in accordance with APP 3.
- metadata should be treated as personal information at least until the final outcome of the *Grubb* proceedings is known.

The release of Pokémon GO caused ripples in Australia and overseas recently when it was discovered that Pokémon GO on iOS requested and was given full access permission to the user's Google account.[1] The controversy prompted the OAIC to issue a statement that it had made enquiries.[2]

The developer of Pókemon GO, Niantic, Inc., responded with an update that limited access permission to basic Google profile information, together with an assurance that no other account information had been accessed.[3]

The incident raises a number of privacy issues. The collection, use and disclosure of player data can be critical to the success of a mobile game, not only in terms of gameplay, troubleshooting and further development, but also in terms of commercialisation through sharing the data with third parties. If the underlying data practices are not compliant with Australian privacy laws, the impact on the valuation of the client's business may be significant.

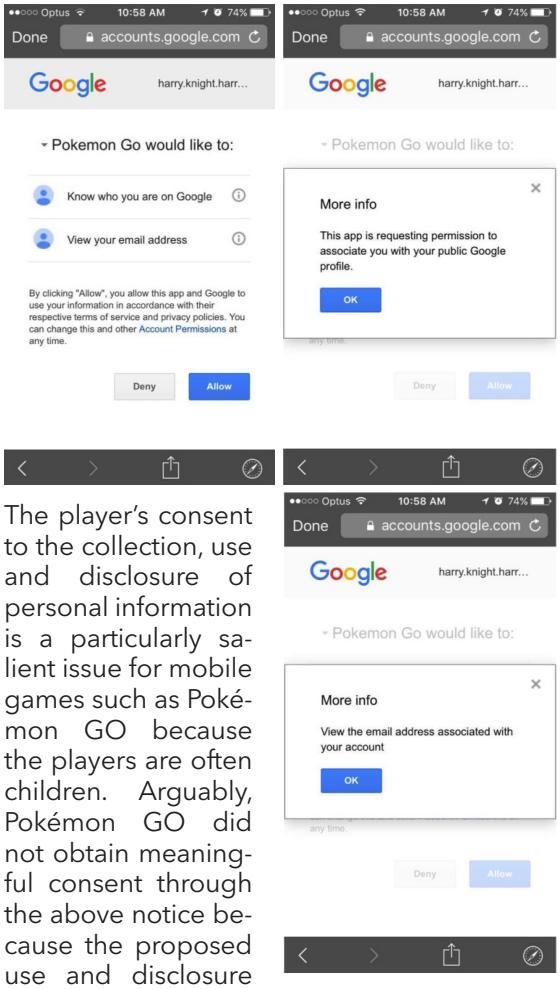
This article will identify and address common privacy issues in the context of big data that Australian practitioners should bear in mind when advising mobile game developer clients.

MEANINGFUL CONSENT

The OAIC released a guide in 2014 entitled *Mobile privacy: a better practice guide for mobile app developers.*[4] The guide is an important resource in advising mobile game developers. In particular, there is guidance on obtaining meaningful consent from players despite the small screen of the mobile device.

The guidance is that mobile games should, amongst other things, use short form notices that summarise the type of personal information that will be collected and the proposed use and disclosure of that information. The guidance in particular mentions that the notice should disclose any third party data sharing practices.

Following the Pokémon GO update, Niantic, Inc. used the below short form notice to obtain player's consent to the collection and use of basic Google profile information.



The player's consent to the collection, use and disclosure of personal information is a particularly salient issue for mobile games such as Pokémon GO because the players are often children. Arguably, Pokémon GO did not obtain meaningful consent through the above notice because the proposed use and disclosure of the information has not been summarised.

REASONABLY NECESSARY COLLECTION

APP 3 prohibits the collection of personal information that is not reasonably necessary for an organisation's functions or activities.[5] According to the OAIC's APP guidelines, an organisation's functions or activities include proposed functions or activities for which the organisation has established plans.[6]

Of course, an "organisation" within the meaning of the APPs does not include entities with

1 e.g. https://www.theguardian.com/technology/2016/jul/11/pokemon-go-privacy-security-full-access-google-account
2 https://www.oaic.gov.au/media-and-speeches/statements/pokemon-go
3 https://support.pokemongo.nianticlabs.com/hc/en-us/articles/222648408-Permissions-update
4 https://www.oaic.gov.au/agencies-and-organisations/guides/guide-for-mobile-app-developers
5 *Privacy Act 1988*, Schedule 1, principle 3.2
6 https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-3-app-3-collection-of-solicited-personal-information

an annual turnover of $3 million or less. This financial threshold would exclude many mobile game developers from the need to comply with the APPs.

The functions or activities of a mobile game developer, including any proposed functions or activities, typically would be the gameplay, troubleshooting and further development of the mobile game. The personal information that is reasonably necessary for such functions and activities would vary. For example, while the player's location is necessary for Pokémon GO gameplay, it would not be necessary for, say, Candy Crush Saga.[7]

According to the Pokémon GO privacy policy, the following information is collected (without limitation)[8]:

- the player's basic Google or Facebook profile information;
- the player's username and the content of messages to other players;
- the player's country and language;
- the player's user settings; and
- the player's location.

This information appears to be reasonably necessary for the functions and activities associated with Pokémon GO. However, the following player information may also be collected:

Internet Protocol (IP) address, user agent, browser type, operating system, the web page that a User was visiting before accessing our Services, the pages or features of our Services to which a User browsed and the time spent on those pages or features, search terms, the links on our Services that a User clicked on, and other statistics.[9]

Not all of this information appears to be reasonably necessary for the developer's functions or activities. In fact, the information appears to be collected as part of the developer's third party sharing practices, which is disclosed in Niantic, Inc.'s privacy policy as follows:

We may share aggregated information and non-identifying information with third parties for research and analysis, demographic profiling, and other similar purposes. This information will not include your (or your authorized child's) [personal information].[10]

Clearly, the Pokémon GO business model includes (or is intended to include) a revenue stream based on sharing data with third parties. This revenue stream may be more important than the revenue stream based on "in-app purchases", or any proposed revenue stream based on "in-app advertising" (which the game currently does not feature).

The question is whether such information is personal information for the purpose of Australian privacy laws.

METADATA

In the Grubb proceedings,[11] the Administrative Appeals Tribunal found that mobile network data in relation to Mr Ben Grubb requested from Telstra was not personal information within the meaning of the then Australian privacy laws.

The Deputy President made the following observation at [112]-[113]:

[112] Had Mr Grubb not made the calls or sent the messages he did on his mobile device, Telstra would not have generated certain mobile network data. It generated that data in order to transmit his calls and his messages. Once his call or message was transmitted from the first cell that received it from his mobile device, the data that was generated was directed to delivering the call or message to its intended recipient. That data is no longer about Mr Grubb or the fact that he made a call or sent a message or about the number or address to which he sent it. It is not about the content of the call or the message. […]

[113] I have considered also the IP address allocated to the mobile device which Mr Grubb used. […] I am satisfied that an IP address is not information about an individual. Certainly, it is allocated to an individual's mobile device so that a particular communication on the internet can be delivered by the Internet Service Provider to that particular mobile device but, I find, an IP address is not allocated exclusively to a particular mobile device and a particular mobile device is not allocated a single IP address over the course of its working life. It changes and may change frequently in the course of a communication. The connection between the person using a mobile device and an IP address is, therefore, ephemeral. [...]

Applying this reasoning to the Pokémon GO scenario, the metadata collected by Niantic, Inc. is unlikely to constitute personal information for the purpose of the APPs.

That said, the decision is currently on appeal to the Full Federal Court. It may therefore be prudent to advise mobile game developers to treat player metadata as personal information until the final outcome of the Grubb proceedings is known. This means that, amongst other things, any player metadata shared with third parties should be aggregated and properly de-identified.

CONCLUSION

Pokémon GO raises common privacy issues in relation to the collection, use and disclosure of personal information. These issues include obtaining meaningful consent, only collecting personal information that is reasonably necessary, and treating player metadata as personal information (at least for the time being). The growing importance of data collection and third party sharing for the monetisation of mobile games means that legal practitioners should be prepared to address these issues when advising mobile game developers.

7 of course, player location may not be "personal information" within the meaning of the APPs - see the section on metadata below.
8 https://www.nianticlabs.com/privacy/pokemongo/en
9 clause 2(c) – Information Related to Use of the Services.
10 clause 3(c) – Information Shared with Third Parties.
11 *Telstra Corporation Limited v Privacy Commissioner* [2015] AATA 991

6 Cyber Security Standards You Need to Know About if You Are a Company Director or Board Member

Sean Field, Special Counsel, Maddocks, provides an overview of the cyber security standards that all Company directors and officers should know about.

INTRODUCTION

By now there can be no doubt that legal obligations on company directors and officers under the Corporations Act to discharge their duties with care and diligence extend into the field of cyber security.

In its Cyber Resilience: Health Check (ASIC Report 429) (the **Report**) the Australian Securities and Investments Commission (**ASIC**) has clearly articulated its position on cyber security and directors' duties, stating that:

- it considers board participation important to promoting a strong culture of cyber resilience;[1] and
- a failure to meet obligations to identify and manage cyber risks may, if you are a director or officer of a company, result in you being disqualified from your role.[2]

As a director or board member, how can you satisfy yourself that you have taken sufficient steps in this regard?

This article provides:

- a concise guide to 6 Cyber Security Standards which you should know about; and
- a six point cyber security check list.

Familiarity with the 6 Cyber Security Standards will:

- give you a basic grasp of cyber security issues in your organisation; and
- allow you to have appropriate conversations with and to ask the questions that need to be asked of your line management with responsibility for IT and cyber security.

The accompanying "Six Point Cyber Security Check List" is intended to provide a high level entry point for Company Directors and Board Members to design strategies to meet their legal obligations in relation to cyber security.

THE 6 CYBER SECURITY STANDARDS

Number 1:
Australian Signals Directorate's Top four mitigation strategies to protect your ICT system[3]

The Australian Signals Directorate (**ASD**) is the Commonwealth's peak advisory body on cyber security.

Its 2012 publication, *Top four mitigation strategies to protect your ICT system,* the ASD sets out four cyber security strategies which it says, if implemented, can address up to 85% of targeted cyber intrusions. These strategies are a subset of a wider suite of ASD's published cyber security strategies.[4]

Number 2:
The Australian Government Cyber Security Operations Centre's Questions Senior Management Need to be Asking about Cyber Security[5]

The Cyber Security Operations Centre (**CSOC**) **is** a joint agency under the responsibility of the Commonwealth Attorney-General and the Minister for Defence.

The CSOC suggests that senior management should be asking the following questions:

- What would a serious cyber incident cost our organisation?
- Who would benefit from having access to our information?
- What makes us secure against threats?
- Is the behaviour of our staff enabling a strong security culture?
- Are we ready to respond to a cyber security incident?
- Has the organisation applied ASD's top four mitigation strategies? (see Number 1, above).

Number 3:
ASIC's Cyber Resilience: Health Check (ASIC Report 429)

For directors and officers of corporations and other ASIC regulated entities, this guidance [ASIC's Cyber Resilience: Health Check (ASIC Report 429)] from the regulator should be compulsory reading.

1 ASIC *Cyber Resilience: Health Check (ASIC Report 429)*, (19 March 2015) available at <http://download.asic.gov.au/media/3062900/rep429-published-19-march-2015-1.pdf> 1, 29

2 Ibid 38.

3 Australian Signal Directorate, *Top Four Mitigation Strategies to Protect Your ICT System* (2012) available at <http://www.asd.gov.au/publications/protect/Top_4_Mitigations.pdf>

4 Australian Signal Directorate, *Strategies to Mitigate Targeted Cyber Intrusions – Mitigation Details* (2014) available at <http://www.asd.gov.au/publications/Mitigation_Strategies_2014_Details.pdf>

5 Australian Government Department of Defence Cyber Security Operation Centre, *Questions Senior Management Need to be Asking about Cyber Security* (August 2012) available at <http://www.asd.gov.au/publications/protect/senior_management_questions.htm>

The Report contains a number of "Health Check Prompts" which provide useful guidance as to the questions directors and officers can ask in assessing their organisation's awareness of and preparedness for cyber security issues.

The Report notes that:

- for listed entities, a cyber attack may need to be disclosed as market-sensitive information; and
- cyber risks may need to be disclosed in Product Disclosure Statements.[6]

Number 4:
The Office of the Australian Information Commissioner's Guide to securing personal information – "reasonable steps" to protect personal information[7] (**the OAIC Guide**)

The Privacy Act 1988 (Cth) requires regulated entities to take such steps as are reasonable *in the circumstances* to protect personal information from misuse, interference and loss; and from unauthorised access, modification or disclosure (Australian Privacy Principle (**APP**) no. 11).

But what constitutes "such steps as are reasonable in the circumstances"?

The OAIC Guide provides useful information in this regard and should be read in conjunction with the other documents referred to in this article.

Number 5:
The Payment Card Industry's Data Security Standard (DSS): Requirements and Security Assessment Procedures (the **PCI Standard**)[8]

If your organisation processes card payments, it should comply with the PCI Standard.

If your organisation outsources card payment processing, your outsourced service provider should comply with this Standard.

Number 6:
ISO/IEC Standards

The International Organisation for Standardisation (**ISO**) and the International Electrotechnical Commission (**IEC**) publish a number of standards used across the IT industry, including specific standards relating to IT security.

The key IT and cyber security standards are the ISO 27000 series.

These are highly technical and detailed publications and it is not suggested that directors and officers become experts in these standards and their implementation.

However directors and officers can ask whether their organisation, suppliers to it and third party products and services are compliant with applicable ISO/IEC standards such as ISO 27000.

Such compliance will not be necessary or appropriate in all cases but to ask these questions may serve as a useful prompt for a discussion with your IT manager or CIO about whether you, your suppliers and third party products are or should be ISO/IEC compliant.

CONCLUSIONS

1. Your organisation's most basic (but arguably not sufficient) cyber-security strategy must include the following:
   a. implement ASD's top 4 cyber intrusion mitigation strategies;
   b. implement the other ASD published strategies, as applicable;
   c. in respect of any of the ASD strategies that are not implemented, ensure that your organisation has a clearly documented audit trail of the reasons why it decided not to implement a particular strategy. That documentation should include an appropriate risk analysis;
   d. ask CSOC's six questions of your IT manager or CIO – are you happy with the answers you get?;
   e. apply ASIC's "Health Check Prompts" to your organisation – what do the outcomes tell you about your organisation's cyber-preparedness?;
   f. if your organisation collects, stores, handles or processes personal information, ask whether it meets the standards set out in OAIC's Guide;
   g. if your organisation processes card payments, ask whether it and its service providers comply with the PCI Standard;
   h. ask whether your organisation, its suppliers and third party products meet ISO/IEC standards, if applicable/appropriate?
2. The 6 Cyber Security Standards referred to in this article and the Six Point Check List below are by no means exhaustive. This article is intended as an introductory guide to allow the non-technical director or officer to ask the right questions of those with managerial responsibility for IT and cyber security.
3. We have not, for example, discussed above the publications put out by the Australian Prudential Regulation Authority (**APRA**). While APRA's publications are aimed particularly at the banking, insurance and superannuation industries, they are of relevance to a wider audience[9].

SEAN FIELD is a Special Counsel at Maddocks, specialising in technology law, intellectual property and M&A transactions in the technology sector.

6 ASIC, see above n 1, 1.

7 Office of the Australian Information Commissioner, *Guide to Securing Personal Information – Reasonable Steps to Protect Personal Information* (January 2015) available at <https://www.oaic.gov.au/resources/agencies-and-organisations/guides/guide-to-securing-personal-information.pdf>

8 PCI Security Standards Council, *Data Security Standard: Requirements and Security Assessment Procedures* available at <https://www.pcisecuritystandards.org/document_library>

9 See for example APRA's *Information Paper: Outsourcing Involving Shared Computing Services (Including Cloud), Prudential Practice Guide CPG 234 – Management of Security Risk in Information and Information Technology and Prudential Practice Guide CPG 235 – Managing Data Risk.*

Six Point Cyber Security Check List for Company Directors and Board Members

1. Has your organisation implemented the Australian Signals Directorate's Top 4 Cyber Risk Mitigation Strategies?

   The Australian Signals Directorate (**ASD**) suggests that implementing ASD's ***Top four mitigation strategies to protect your ICT system*** can address up to 85% of targeted cyber intrusions.

2. Ask your CIO the Cyber Security Operations Centre's ***Questions Senior Management Need to be Asking about Cyber Security:***

   a) What would a serious cyber incident cost our organisation?
   b) Who would benefit from having access to our information?
   c) What makes us secure against threats?
   d) Is the behaviour of our staff enabling a strong security culture?
   e) Are we ready to respond to a cyber security incident?
   f) Have we applied ASD's top four mitigation strategies?

3. **Take the ASIC "Cyber Resilience Health Check"**

   ASIC's ***Cyber Resilience: Health Check (ASIC Report 429)*** contains a number of "Health Check Prompts" and provides useful guidance as to the questions directors and officers can ask in assessing their organisation's awareness of and preparedness for cyber security issues.

4. **Does your organisation collect or handle personal information? If so is it compliant with the *Privacy Act 1988* (Cth)?**

   Does your organisation meet the legal requirement to *take such steps as are reasonable in the circumstances* to protect personal information from misuse, interference and loss; and from unauthorised access, modification or disclosure (Australian Privacy Principle (**APP**) no. 11)?

5. **Does your organisation process card payments?**

   If so, is it (or its card payment processing service provider) compliant with the Payment Card Industry's *Data Security Standard (DSS): Requirements and Security Assessment Procedures*?

6. **Are your organisation and its outsourced services/service providers compliant with applicable industry standards? Are third party products used in your organisation compliant?**

   For example, the ISO 27000 series of IT and cyber security standards published by the International Organisation for Standardisation and the International Electrotechnical Commission. See ISO/IEC 27018:2014; ISO/IEC 27001:2015.

Sean Field, Special Counsel, Maddocks

Privacy, Data & De-identification

Acting Information Commissioner Timothy Pilgrim delivered this speech to CeBIT in Sydney on 2 May 2016.

Good afternoon.

I acknowledge the Wanngal people as the traditional custodians of this land, and pay my respect to elders past and present. I also thank CeBit for inviting me to speak to you today.

data is core to the development and delivery of most services, to paid and unpaid activities across the economy, and to better quality public policy

Today, I'm here to discuss privacy, data, de-identification; and the opportunities these present in an Australian context.

And the opportunities of bringing these three issues together in an integrated way are, I believe, significant – for Australian Government agencies and Australian businesses.

In fact, the raw potential that big data presents to both public and private sector alike is so extraordinary that it's a little hard to explain in words.

Yet a mathematician came close, in my view, and did so 202 years ago.

It's with a little trepidation that I refer to the works of great pioneering mathematicians in front of a CeBit audience, but those amongst you with a taste for the classics may recall "LaPlace's Demon".

This was Pierre-Simon LaPlace's famous treatise on determinism, which is often crudely summarised as the theory that if one could know the location and velocity of every object in the universe at a given point, one could predict the rest of history.

If that crude summation of LaPlace sounds suspiciously like history is throwing down a gauntlet to the power of big data analytics, then his actual words are even more prophetic:

> *We may regard the present state of the universe as the effect of its past and the cause of its future.*
>
> *If an intellect could know all forces that set nature in motion, and all positions of all items of which nature is composed, and* ***if this intellect were also vast enough to submit these data to analysis,*** *then nothing would be uncertain.*
>
> *The future, just like the past, would be present before its eyes.*[1]

Today we might simply quip that past metadata is the best predictor of future metadata.

But either way, the power of data-based prediction, which LaPlace could only theorise about, is now a reality.

Big data has changed the way we identify trends and challenges, as well as identify opportunities. As a result, it has the potential to bring about enormous social and economic benefits.

Trends drawn from big data can be used to personalise individuals' experiences, to target products and services, to improve health management, crime prevention, and emergency responses.

We've seen big data used not only to predict natural disasters, like flooding and earthquakes, but also to respond to them.

In 2015 the Humanitarian Data Exchange was used to help relief efforts following the Nepal earthquake. A task force of about 2,000 people from 80 countries analysed 'millions of Nepal-related tweets to build several databases'. This data helped produce quick-and-dirty maps to coordinate efforts by the government, the UN, and NGOs.[2]

And as the amount of data is growing exponentially, that potential can only increase.

As the Productivity Commission's recent Issues Paper explains, 5 billion gigabytes of data was the amount of data generated worldwide in the year 2002. We now generate it *every two days*.

And when I say "we", I mean it truly is a global community effort.

When we wake up, we check Twitter or Facebook or our emails.

Over breakfast we use our iPads to read the news.

Before work we might fit in a quick session at the gym – our Fitbit tracking our progress.

As we head off to work our smart phone pings the towers along the way.

Swiping our work pass we enter the building before logging onto our computers.

With each step we take we are, quite literally, creating more and more data – potentially revealing more and more about ourselves.

1 *Pierre Simon Laplace, A Philosophical Essay on Probabilities*

2 *How The Candy Crush Of Data Is Saving Lives In Nepal*

And as our digital touch points increase, and the Internet of Things becomes more and more embedded in our everyday lives, the data we create becomes increasingly valuable.

Valuable to both private and public sector alike.

The Prime Minister made this clear when he released the *Australian Government Public Data Policy Statement* at the end of last year. It recognises data held by the Australian Government as a strategic national resource that holds considerable value for growing the economy, improving service delivery and transforming policy outcomes for the Nation.

This priority is reflected in the fact that the Prime Minister's own department has established a Public Data Branch to lead data innovation across the public service.

After all, the policy and service delivery improvements that can be yielded if this national resource can be shared and built upon are immense.

Accordingly, the Productivity Commission has been tasked with looking at *Data Availability and Use*. In its Issues Paper, the Commission argues that data is core to the development and delivery of most services, to paid and unpaid activities across the economy, and to better quality public policy.

Both of these key Government papers *also* make it clear that upholding the highest standards of data security and privacy are *critical*. And I welcome this focus.

Because my Office, the Office of the Australian Information Commissioner, has long supported the view that public information is a national asset.

Indeed, the FOI Act, which we administer alongside the Privacy Act, explicitly describes government information as a national resource.

We understand that the potential of that resource may be best realised when data can be shared, used and built upon.

But we also understand, and hope is evident, that this can only occur sustainably, if privacy is integral to the equation.

Simply put, a successful data-driven economy needs a strong foundation in privacy.

Our experience and community research shows that by and large people do want their personal information to work for them, provided that they know it is working *for* them. When there is transparency in how personal information is used, it gives individuals choice and confidence that their privacy rights are being respected.

Accordingly, good privacy management and great innovation go hand in hand.

Because when people have confidence about how their information is managed, they are more likely to support the use of that information to provide better services.

In fact, their expectations often become entirely supportive.

Most people *do* expect organisations to use their information where it's necessary to provide them with the services they want or to improve on those services.

They do expect law enforcement agencies to use information resources to stop crime and to keep people safe.

However, people also want to know how their information is being used, who has access to it, and what that means for them in terms of their personal identity.

Accordingly, privacy law – often misunderstood to be about secrecy, is really underpinned by transparency and accountability.

Accordingly, good privacy management and great innovation go hand in hand

And by ensuring organisations are transparent and responsible when handling personal information, privacy management strengthens customer trust.

Building this trust is key to our big data challenges – whether sought in the form of customer confidence or political mandate.

As the Chairman of the Productivity Commission has said 'the significant evolution in data collection and analysis seen in recent times suggests that the culture, standards and policy structures that have been applied to big data analytics may need to move out of the back room and into the showroom if community confidence and wide opportunity for innovation are to be maximised.'

And I agree.

We know from my Office's longitudinal surveys into community attitudes to privacy, that Australians are becoming increasingly conscious of personal data issues.

The majority of Australians – 60 percent – have decided not to deal with an organisation due to concerns about how their personal information will be used. And significantly, 97 percent of Australians don't like their personal information to be used for a secondary purpose.

This is critical to big data. Because big data projects will often involve secondary use of data.

If that data finds its source in personal information, then we have a clear dissonance between our known and understandable desire that our personal information works *for us* and for the purposes *we* explicitly provided it for versus the demonstrable innovative power of that data to improve our services and lives.

Addressing this dissonance will require a multi-pronged approach.

Part of it will lie in making the case as to how, through secondary uses, our personal information is still clearly working for our benefit, either directly or communally – and numerous research fields point to the potential to make this case.

De-identification is a smart and contemporary response to the privacy challenges of big data

Part of it will lie in greater security and protection of the personal information – and a determined approach to counter would-be disrupters of our national data resource – as the Government's new *Cyber Security Strategy* reveals.

But part of the solution, and potentially a significant part I suggest, lies in getting de-identification right, and right such that government agencies, regulators, businesses and technology professionals have a common understanding as to what "getting it right" means.

At the moment, that common understanding is not evident.

I know, for example, that when I've previously spoken about precautions with *anonymised* data sets the result has been reporting that I'm advising to treat *de-identified* data as personal information.

This would be illogical advice at best, because correctly de-identified information is, by definition, no longer personal information.

To be clear, this has never been my Office's view, but the example highlights the current haze around this issue and the need to obtain an agreed understanding.

There may well be people in this room who are thinking, "well, I understand the distinction between anonymised and de-identified just fine thank you" and I'm sure that's true.

But as per the Productivity Commission's point, we need to move this knowledge out of the backroom and in to the showroom in order to build public confidence in this potential privacy solution.

Because it *is* a potential solution.

De-identification is a smart and contemporary response to the privacy challenges of big data – using the same technology that allows data analytics to strip data sets of their personal identification potential, while retaining the research utility of the data.

When done correctly, de-identified information is no longer personal information and is therefore outside the scope of the *Privacy Act*.

But what does "done correctly" entail?

De-identified means de-identified in *whose* hands?

And in *what* use?

If I am the collector of the personal information, am I obliged to have regard to the re-identification potential of data in its *current* context, the next *foreseeable* context, or *any* context?

And what about the ability of data analytics to create entirely new and personal information – raising the prospect of an entity effectively collecting new personal information by creating it?

These are all pertinent questions, but if you think I'm going to give clear and simple answers now, then I'm afraid you are in for disappointment.

This is for a good reason. Namely, the *Privacy Act* is principles, not prescription, based, and ultimate answers as to compliance with it will often be bespoke to the circumstances.

This is certainly true if your preferred solution to privacy governance is de-identification. The specific changes required to your data set will arrive as the result of a risk based assessment of the data's potential use, disclosure and re-identification prospects.

While the principles remain constant – and are already covered in our existing guidance on information sharing and de-identification – the solutions executed are often bespoke to the data and its intended use.

This is why it's not desirable to try and provide a prescriptive, template based, tick-a-box guide to de-identification.

It is why, despite already having guidance in this space, we will be opening up consultation on renewed guidance this year.

Because it is clear from the speed at which this big data is evolving that any privacy solution which is *purely* regulator-driven, without the voice of industry, consumers and government agencies to inform it, will not serve our purposes here.

To be clear, the *Privacy Act* principles, and the accountability of my office to regulate them, are both established, clear and ongoing – but ensuring that the application of these regulatory principles is as practical as possible in real world examples, is of benefit to both regulator and regulated alike.

This was the primary point of my recent, perhaps wistful, comparison between our current national race to harness the potential of big data, and the technological pioneering of the moon race.

As was the case with *that* great technological goal, potential solutions to balancing the democratic, strategic and commercial benefits of big data will lie in a multi-sector co-operation.

The OAIC understands that this is an area of regulation where agreed industry terms and standards will be critical – not only to the actual efficacy of de-iden-

tification, but also to provide public confidence in it as a solution.

After all, infamous and widely publicised examples of 're-identification' by white hat hackers and journalists already create an impression of de-identification as a flawed solution.

Yet on deeper analysis these are, almost exclusively, examples of so called 'de-identifications' that were not conducted to any known industry standards.

They are therefore not arguments *against* de-identification as a privacy solution, but arguments *for* getting it right, with agreed industry standards, checks and balances, audit and review, and quality control built in to your processes.

Because the track record of *expertly* de-identified data preventing data breaches is strong. Resolving the nexus between privacy and big data is therefore a goal my office needs to reach in partnership with the sectors that are broadly represented by the people in this room; and my office will be commencing a national conversation to achieve this goal this year.

It will start shortly with the release for public consultation of new draft guidance to utilising big data in an Australian privacy law context.

This will be followed by a series of engagement opportunities with both public and private sector focus, promoted through our Privacy Professionals Network.

The purpose of our discussions will be to test our draft guidance with business, technical, legal, academic, policy and community sectors – and it is my goal that this time next year, I will speak to CeBit 2017 with a shared understanding for both businesses and agencies on de-identification as a privacy-enhancing tool.

I stress that de-identification is not the only approach available to manage the privacy dimensions of big data, but it is one with powerful potential, when done fully and correctly.

That potential includes the ability to facilitate data sharing between agencies, unlock policy and service gains of big data innovation, and support the Internet of Things whilst protecting the fundamental human right to privacy.

That is a great prospect, one that we should realise together, and we look forward to working with you to achieve.

I hope I have conveyed to you that my office understands the great public potential of big data, as well as why integrating this with individual privacy remains critical.

But, if my bureaucratic prose has failed then, having opened with LaPlace, let me close by reflecting on the words of another prophetic soul, albeit a fictional one; Sam Seaborn, of *The West Wing*.

In an episode first aired in 1999 he argues that, just as the 20's and 30's were defined by debate on the role of government, and the 50's and 60's by civil rights, the arrival of the information age would place privacy as a central issue of law and government in the 21st century.

Perhaps the writers were prescient, but then our individual privacy has always been essential to our individual freedom – to our right to have autonomy as to how we shape our lives and move in the world.

And, as the ever-erudite Mr Seaborn notes; *"In a country born on the will to be free, what could be more fundamental than this?"*

One can say the same of course for any free and democratic nation, ours being one.

the Privacy Act is principles, not prescription, based, and ultimate answers as to compliance with it will often be bespoke to the circumstances

While there is great societal benefit in liberating the potential of our information assets, community confidence will be tied to transparent protection of our own individual liberty – in the form of knowing who knows what about us.

Smart privacy solutions and smart data solutions are therefore not mutually exclusive, nor elusive, but mutually supportive.

Because with public confidence obtained, the public potential of big data can be fully, and publicly, realised.

Thank you.

VALE Gae Pincus

CAMLA is sad to report the death on 7 August of long-time member Gae Pincus. Gae was a member of CAMLA for many years and a regular attendee of seminars and AGMs. In my time as Administrative Secretary of what was the Australian Communications Law Association (ACLA) and later CAMLA, Gae kept up her membership and her support of CAMLA with admirable loyalty. She first became a CAMLA member in the early 1990s when she was working for the OTC (Overseas Telecommunications Commission) and then in Canberra for the National Food Authority as foundation Board Chair and CEO. In the late 1990s she became Chairperson of the Energy Industry Ombudsman NSW, a nice segue from food to energy! Gae was also on the management committee and then the Board of the PIAC in the 1990s. In all of these roles she was a tireless advocate for the public interest and a policy maker of great social conscience. She was the Chair of the Communications Law Centre (CLC) from the late 1990s until her death, and oversaw the transition of the centre from UNSW to Victoria University (where it had a association) and then to UTS. Her illness did not stop her wanting to participate and she conducted her last CLC board meeting via teleconference from her bed at home.

I knew Gae as a strong supporter of CAMLA and of my role as administrative secretary. She understood well the importance of keeping a membership such as CAMLA's active and the tasks that involved. Her experience working with "start up" organisations gave her great insight into how things happened and who made them happen. She was always one of the first people to renew her membership each year, and always with a cheque, made out in her neat handwriting. As a matter of principle she refused to pay by credit card (I am not sure that she even owned one!) and she certainly did not use email in the time that I was administrative secretary. Her knowledge of policy and the law was at its finest when she was part of a team at the CAMLA Cup.

For many years Gae and I were neighbours in Glebe, and would often meet on the street or on the bus. I always enjoyed her company and our conversations about what was going on in our world. I admired her as a strong independent woman with a social conscience and a dry wit, never afraid to speak her mind. A great role model.

Ros Gonczi
29 August 2016

Please join the Centre for Media Communications Law (CMCL), Communications and Media Law Association (CAMLA) and Corrs Chambers Westgarth for an invite only morning seminar in Sydney with special guest CMCL visiting scholar John Battle, Head of Compliance at ITN in London.

Date: **Wednesday 14 September**

Time: **9:30am – 12:00pm**

Where: **Corrs Chambers Westgarth, Level 17, 8 Chifley, 8-12 Chifley Square, Sydney NSW 2000**

Registration is essential – Please RSVP by Friday 9 September to law-cmcl@unimelb.edu.au

UK Media Law - Recent Developments

The first session will focus on the Defamation Act 2013 (UK) and its aftermath, including the impact that this important reform has had on media reporting. This session will also examine emerging issues in privacy law and the rise of data protection. The second session will consider key developments in the law of open justice, including new court reporting restrictions and cameras in the courts, along with developments in police access to journalists' source information.

John Battle is a leading media lawyer in the UK. He is the Head of Compliance at ITN which produces television news and current affairs programmes for ITV, Channel 4 and Channel 5. He advises journalists on legal and regulatory issues both pre and post broadcast. His specialist areas are contempt of court/ open justice, defamation, copyright law and privacy/ confidentiality. He previously worked as a lawyer for two leading newspaper publishers: Associated Newspapers and News UK. He is the chairman of the Media Lawyers Association and is a member of the Parliamentary and Legal Committee of the Society of Editors. He has been involved in many media law developments such as cameras in court, disclosure of prosecution evidence to the media and greater access to sports footage to news organisations.

Melbourne Law School

T: +61 3 8344 8957 | **F:** +61 3 9348 2353 | **E:** law-cmcl@unimelb.edu.au
W: http://www.law.unimelb.edu.au/cmcl/ | **W:** (Law School): http://www.law.unimelb.edu.au

CAMLA YOUNG LAWYERS SPEED MENTORING EVENING

Wednesday 19 October 2016

After the success of the event since its launch in 2014, the CAMLA Young Lawyers Committee Speed Mentoring Evening will return in 2016. The event will provide an opportunity for young lawyers to meet leading lawyers from the media and communications industry.

SAVE THE DATE

Wednesday 19 October 2016

Baker & McKenzie, Level 27, 50 Bridge Street Sydney

More details will be provided closer to the date

Tickets will be limited so register your interest now by emailing **camla@tpg.com.au**

CONTRIBUTIONS & COMMENTS

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

Contributions in electronic format and comments should be forwarded to the editors of the Communications Law Bulletin at clbeditors@gmail.com

ELECTRONIC COMMUNICATIONS LAW BULLETIN

CAMLA is pleased to offer our members the Communications Law Bulletin in electronic format.

Please contact Cath Hill: camla@tpg.com.au or (02) 4294 8059 to indicate your delivery preference from the following options if you have not done so already:

☐ Email ☐ Hardcopy ☐ Both email & hardcopy

About CAMLA

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

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

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

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

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

Disclaimer

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

For further information:

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

To: The Secretary, camla@tpg.com.au or CAMLA, 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)

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

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

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