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!