GILBERT +TOBIN

# GILBERT + TOBIN INNOVATION INSIGHTS

FINANCIAL REVIEW

AUG 2016

WWW.GTLAW.COM.AU

# CONTENTS


WELCOME TO THE AFR 2016 INNOVATION SUMMIT 3

DATA AND THE INTERNET OF THINGS 4

IP IN A DIGITAL WORLD THINKING INSIDE THE BOX 7

ROBOTICS AND AUTOMATION 9

FINTECH: DATA MONETISED AND MONEY DIGITISED 12

BLOCKCHAIN AND SMART CONTRACTS: DIGITAL UTOPIA VERSUS THE REAL WORLD 13

ACCC TOUCHPOINTS IN THE DIGITAL ECONOMY 16

CYBERSECURITY 18

MAKING THE MOST OF YOUR DATA GETTING DATA ANALYTICS CONTRACTS RIGHT 21

INNOVATION IS IN OUR DNA 26

ABOUT GILBERT + TOBIN 27




GILBERT +TOBIN

# WELCOME TO THE AFR 2016 INNOVATION SUMMIT


## THERE IS NO DOUBT THE BUSINESS WORLD IS EVOLVING RAPIDLY, AND GILBERT + TOBIN IS COMMITTED TO DEVELOPING INNOVATIVE SOLUTIONS FOR CLIENTS AND OFFERING MUCH MORE THAN STRATEGIC LEGAL ADVICE.

The global economy is undergoing profound changes that many are calling a 'Fourth Industrial Revolution'. This **technology-driven revolution**, like those before it, is being driven by increased automation and connectivity.

These changes will have significant implications for national economies and a range of industries and the players within them. New competitive models, companies and sectors will emerge. Cost bases will change as labour-intensive industries adopt cheaper robots or **intelligent software**. Intermediaries will be replaced by technologies, such as blockchain.

Considerable economic activity and strategic adjustment will result:

+ incumbent companies will seek to adopt the benefits of automation and digitisation into their core operations, seek new sources of growth in adjacent areas and take steps to deal with disruptive entrants;
+ new companies will emerge that utilise new technologies to attack the business models and profitable areas of existing incumbents; and
+ government and regulators will need to deal with policy issues and adapting regulation to deal with new forms of business.

These changes will provoke a range of legal issues: new forms of contracting and alliances; the development and protection of new types of often intangible assets; different and often globalised competition issues; dealing with regulations that have not anticipated the emerging technologies; and entirely new technologies.

At Gilbert + Tobin we are working on the answers to all of these issues. For many of our clients we are the trusted advisor and execution partner in a way that significantly transcends the role of a traditional legal partner. Some of technology impacts we are dealing with are referenced in the articles in this booklet. These are a snapshot of what our market leading partners are thinking about, and I would encourage you to contact our team to discuss how we can assist you with **transformational business projects**.

# DATA AND THE INTERNET OF THINGS

PETER LEONARD PARTNER, TECHNOLOGY, MEDIA + TELECOMMUNICATIONS

## DATA IS AT THE HEART OF THE INTERNET OF THINGS (OR "IOT" - ALSO KNOWN AS THE INTERNET OF EVERYTHING).

Management of data handling, data analysis and data sharing between business entities is a core issue in most IoT services. It's also critical to the operation of IoT communications platforms and the sensor, communication, control and reporting devices used in IoT services.

Diverse data capture, multiple data flows and substantial value-add by data analytics are the essence of IoT services. More and better data creates significant opportunities for most businesses. It also brings disruption of many existing businesses and new sources of business risk. The opportunities afforded by IoT come with risks and challenges. Many are entirely novel and require the development of new business models, laws and new forms of contract.

At its most basic, the "IoT" refers to the concept of connecting any device with an on and off switch to the Internet and other devices. An IoT device may be any device capable of connection, including everything from vehicles, smartphones, thermostats, kettles, swimming pools, washing machines, headphones, lamps, wearable devices and so on. The IoT also encompasses remote monitoring of machines and their components (such as an electricity network or the jet engines of an airplane) and remote operation of machines (such as mining vehicles or undersea craft).

Many IoT services incorporate sensor devices. These sensors may be passive devices that monitor and report on conditions in a particular environment, or active (actuator) devices capable of changing and controlling conditions in that environment.

IoT services may be machine-to-machine as well as human-to-machine. Some IoT applications provide consumers with information that enables them to make decisions based on analysed information (for example, 'smart home' applications to turn on an air-conditioner, to turn off a pool filter or to order chemicals required to treat a swimming pool). Other applications may fully control and adjust conditions in a particular environment without any active consumer intervention. For example, smart home applications that respond to an extreme weather event such as a heat wave by automatically activating sprinklers, closing curtains, turning off non-essential electrical appliances and turning on an air-conditioner in a pet area.

Right now, IoT is probably near the peak of the technology hype cycle. That said, Macquarie Equities (in their July 2016 report '*I Robot, Who can win from digital disruption*') identifies "four mega trends" with the largest potential to disrupt the Australian corporate landscape over the next decade. These are virtual reality, wearables, big data and IoT. Cisco Systems estimates that IoT will increase US corporate profits by 21 per cent in the next eight years, through higher asset utilisation, higher labour productivity, lower waste, improved supply chain logistics, new customers from improved product experiences and reduced the time to market for innovations. Macquarie Equities also suggests that the increasingly rapid business impact of technological change means the opportunity cost of businesses being slow to adopt technologies will rise exponentially.

Technological factors are also converging to escalate the pace of IoT deployment. These factors include:

+ rapid reductions in the cost consumption of sensors coupled with improvements in sensor capacity, durability, robustness and power efficiency;
+ improvements in communications technologies between sensors, hubs and control devices, including 'meshed networks' and other improvements in bandwidth utilisation and reliability;
+ improvements in encryption and other technologies to protect the security of data at rest and in transit,
+ rapid uptake of smartphones, enabling near ubiquity of a relatively low cost and globally standardised device (subject to mobile network availability and wifi coverage), enabling its use as an actuator device and allowing insights to be delivered to users via that device;
+ rollout of cloud-based data warehouses and cloud-based analytics platform services, enabling interconnectivity of services and low cost set-up and tear-down of data sources and analytics capabilities; and
+ rollout of broadband and narrowband networks and IoT platforms and hub devices that support third party IoT services. Many low cost IoT smart home applications require access to an IoT hub device, such as a Nest device, supplied by a third party (eg the consumer).

Third-party supplied devices are integral to the IoT service delivery chain. For example, a smart home application may communicate with service providers via the Nest platform, bought and installed by the consumer and controlled via an app on a the consumer's smartphone or tablet. The variety of device and service options may lead to issues concerning responsibility for failures in service provision caused by third party-supplied devices, communications platforms or carriage services.

Data errors, omissions or breakdowns may also lead to incorrect decisions being made in reliance upon data analysis that is correctly carried out but is based on incorrect or partial data. Sensor-based services may depend on proper operation of third party devices. Since some operating issues can't be detected remotely, an IoT service provider may be unaware of data quality issues affecting the reliability of its service even if it is diligent in real-time service quality monitoring.

Clearly, data quality is important to ensure that IoT services are reliable and accurate. Many IoT applications draw upon one or more external data sources to bring together various inputs for analysis and provide outputs that either make a decision autonomously or present information enabling a human user to make a decision. Making data available for diverse applications creates legitimate concerns about legal liability for data sources, including public sector entities, that capture, curate or make available that data. Many data sources will be concerned that raw data may be incomplete, intermittently available or otherwise unreliable. This may make them unwilling to release that data without quality assurance.

Concerns about exposure arising through data capture and availability may also deter prospective users of IoT services from making their data available. For example, a farmer may be concerned about possible use by environmental activists or environmental regulators of on-farm data that the farmer contributes to an IoT service, or by commodity brokers or traders to gain an advantage in price negotiations with the farmer.

Concerns about data quality and potential legal liability arising are particularly likely to limit the release of data sets by government agencies. Many governments around the world have stated their commitment to release of public data wherever practicable, implementing policy that public data should be a public good. Despite this, access to open government data will be impeded unless liability exposures arising from data quality issues or reliance by users are appropriately assessed and mitigated. Many applications of government data may not be anticipated by the government agency that captures, curates or makes available that data. Uses often involve

creative combination and comparison of multiple data sources. Consider an agricultural IoT service enabling a farmer to make decisions based on a 'dashboard' report providing analysed data outputs ('insights') on the farmer's smartphone. This service may combine data from field sensors measuring moisture content in soil and on plants, meteorological data provided by the Bureau of Meteorology, soil maps and river hydrological data from state agriculture agencies, and on-farm soil analyses by agronomy service providers. These data may be combined with third party material enabling annotations and other value-added features and functions. Or, meteorological predictions may be used to make machine-driven decisions about climate control. Failures or other errors in any of these data sets may compromise the information base and quality of analysed data outputs.

Providers should also consider the impact of privacy laws. Release of data that has been de-identified but not fully anonymised (and so remains vulnerable to concerted re-identification attack) may lead to individuals becoming reasonably identifiable. In such cases any disclosure of this de-identified information could be classed as a release of personal information. Mitigating this risk means controlling the activities of those with access to data about individuals through the deployment of reliable contractual, operational and technical safeguards.

For businesses, additional risks arise from current uncertainty about the status of legal recognition and protection of proprietary rights in data in Australia and other jurisdictions. Current measures may not be completely effective to enable appropriate control over downstream uses of data. Equitable doctrines concerning the protection of trade secrets or confidential information may not be adequate to protect sharing of 'commercial-in-confidence' data as required for many IoT services. This is a particular concern where an IoT service provider is not vertically integrated and relies upon other entities to provide some elements of an IoT service within the IoT service delivery chain.

Particular business risks include:

+ contractual protections as to uses and disclosures of data may not be enforceable against third parties (entities who are not parties to the contract with the data source) - especially since service providers are currently able to move data to jurisdictions with inadequate contract law systems and enforcement frameworks;
+ release of data to facilitate research may compromise protection of this data as confidential (trade secret) information;
+ loss of control of data may directly and adversely affect the business of the data source (for example, data may be used by competitors to target the data source's products, services or customers more effectively);
+ IoT service delivery chains and inter-working of IoT services with IoT communications services and devices, particularly services and devices supplied or managed by third parties, may create security vulnerabilities and weak points where data may be compromised or intercepted; and
+ regulators or litigants may obtain access to the data for uses adverse to the business.

Concerns about loss of control of data or about information security may significantly impede data sharing and provision of open IoT platforms and devices. Unless these concerns are adequately addressed, a likely outcome will be to advantage fully integrated IoT service providers, closing out opportunities for specialist or niche providers. Effective and predictable legal protection (in Australia and in other markets) that facilitates data sharing within the IoT service delivery chain is likely to be more important to Australian start-ups and other Australian businesses than to vertically integrated global operators that provide 'closed system' IoT services.

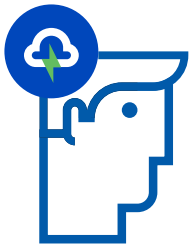
The sharing of data between multiple entities (for example, a data analytics services provider, a communications service provider, a device provider, a data warehouse operator, and so on) also requires sensitivity to consumer concerns. Consumers are concerned about the collection and use of their personal information, but their concerns do not begin and end with data privacy. IoT applications require consumers to trust in the proper and sensitive handling of their information throughout the supply chain. Maintaining that trust is partially enabled by good privacy management, including appropriate transparency and understanding of information handling practices.

Consumers will likely soon demand greater transparency than has been expected to date about how businesses are using data. For example, they may demand information about the pricing of services offered to different customer segments or classes of users, or about disclosures to law enforcement agencies or private litigants. At the same time, although IoT services are becoming more complex and diverse, product lifecycles shortening and the number and range of participants in the IoT service delivery ecosystem are increasing, businesses and consumers are demanding simpler forms of contract and more readily understandable consumer protection laws.


# IP IN A DIGITAL WORLD THINKING INSIDE THE BOX

JOHN LEE, PARTNER, INTELLECTUAL PROPERTY

**BY DEFINITION, TODAY'S INNOVATORS ARE PUSHING THE BOUNDARIES IN TECHNOLOGY, BUSINESS AND SOCIAL INTERACTIONS. IN THE PROCESS, SOMETIMES EVEN WITHOUT REALISING IT, THEY ARE CREATING INTELLECTUAL PROPERTY. THEY ARE ALSO POTENTIALLY RUNNING UP AGAINST OTHERS' IP.**



ANY BUSINESS THAT IS TRULY INNOVATING OR CHALLENGING INCUMBENTS HAS SOME DECISIONS TO MAKE.

WHERE ON THE IP SPECTRUM DO THEY SIT?

WHAT STEPS DO THEY TAKE NOW TO CLARIFY THEIR STRATEGY AND FUTURE-PROOF THEIR BUSINESS?

The question for innovators is how should they factor Intellectual Property (IP) into their planning? As with most business decisions there are a range of responses and the appropriate strategy for a particular business depends on its nature and trajectory. IP strategies range along a spectrum from:

+ a passive approach in circumstances where IP is considered low value, low risk and strategically insignificant; to
+ an active, aggressive IP strategy where IP is seen as essential to the future growth and success of the venture.

At the more passive end of the spectrum might be a mature business in a sector which does not rely on product differentiation or significant investment in innovation. In that environment, having IP as a central strategic plank or a major investment category does not make a lot of sense. At the more active, aggressive end might be a growth-stage business investing significantly in innovation or a large business focussing on product differentiation in a competitive market. For those businesses, a well thought-out IP strategy should be a core part of their overall business strategy.

While the concept of adopting an appropriate IP strategy for a venture is not new, the game changer is the nature and pace of change. The 'fourth industrial revolution' is the era of intangibles. Current business strategy and growth is increasingly skewed towards ideas, concepts, digital assets and services. In a world where the major retail banks consider themselves to be technology companies, and you can build a billion dollar business in a few years based on 'digital hitchhiking', the world is less focussed on physical assets. What, then, is the value that underlies these new world ventures? It's about the IP.

Any business that is truly innovating or looking at new ways to challenge the incumbents has some decisions to make. Where on the IP spectrum do they see their business and their opportunities for growth? What steps do they take now to get some clarity around their strategy? How do they position themselves to ensure they are future-proofed?

A way to start is to spend some time thinking 'inside the box'. Asking: what is it we do differently, better, more efficiently and effectively than others? The answers to these questions help identify the core differentiator of the venture (and it is often not what was initially thought) and assist in deciding what path the venture should take. If the vision is based around competing efficiently on price in a commoditised market, then building around IP is going to be a low priority. On the other hand, if the heart of the business is a new, innovative but readily replicated product, then IP should be a central consideration.

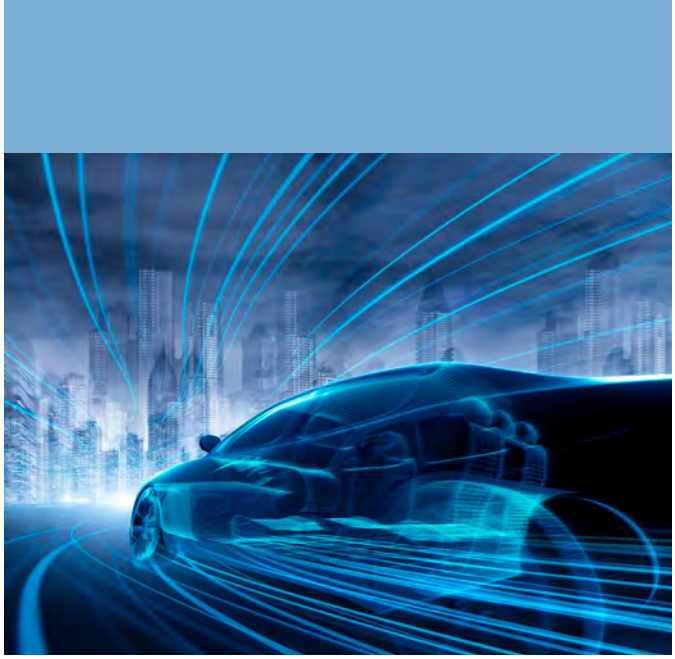
In this process, the venture should get input from a broad cross section of its people. In many cases it is an oversight to leave it to the lawyers or finance team—technology and marketing functions are critical.

Although the fundamentals of IP strategy remain constant, in a rapidly changing world businesses must adapt and adjust constantly to thrive in the new environment.

# ROBOTS AND AUTOMATION

SIMON BURNS, PARTNER,
TECHNOLOGY, MEDIA + TELECOMMUNICATIONS

**WHEN SOPHISTICATED DATA ANALYTICS COMBINES WITH MACHINE LEARNING, THE INTERNET OF THINGS AND ADVANCED ENGINEERING AND MECHANICS, YOU CAN AUTOMATE ALMOST ANYTHING. AUTONOMOUS SYSTEMS OR ROBOTS – WHETHER PHYSICAL OR VIRTUAL – BRING IT ALL TOGETHER.**



## WHEN CONSIDERING AUTOMATION, THE BIG QUESTIONS ARE:

**CAN WE DO IT?** Are automated cars allowed on the road? Are we allowed to let a computer give personal financial advice? Are we allowed to use an app to diagnose skin cancer?

**WHO IS LIABLE?** What if it crashes? What if it gives the wrong advice? Are we at fault?

## CAN WE DO IT?

The pace of technological advances in business make it tempting to "just do it" and ask questions (or forgiveness!) later. Even in today's high velocity business world, though, you need to understand the risks first.

Given what is achievable today, it should be rare that a sophisticated automated solution cannot meet regulatory requirements. The real question is: how does it need to operate to meet those regulatory requirements?

Assessing whether regulations permit a robotic or automated solution requires a very good understanding of what is possible with machine learning and artificial neural networks as well as deep expertise in the regulatory environment and the law. There are many examples of lawyers and regulators saying "no, you can't" based on an incomplete understanding of the sophistication of automated solutions.

So, the first step is to find someone who gets both the technology and the law - and find them before you have built the thing! Only then will you get good advice on whether your new innovation is likely to run in to regulatory hurdles and how it can developed to operate in a compliant manner.

Do this before you cut the code, as the best solutions are "compliant-by-design". Think about the learning model, think about auditability of decision-making, think about guidance models, customer filtering and manual overrides.

It's also important to understand precisely what you are trying to achieve with the solution. Many clients and regulators start with a misconception that the product needs to be perfect, that it needs to anticipate and solve all issues in all scenarios. That is clearly difficult, and also not required. A better approach is set a baseline of the current manual solution and then focus on what the new automated solution needs to do to be an improvement. For example, in financial advice contexts, "robo-advice" solutions don't need to deal with all risks within the industry. Of course, there will always be risks that the advice given is wrong or that the solution does not act in the client's best . However, these risks exist today with the human solutions.

It is important to set this baseline and understand the incremental risk to your business. The ability to define parameters and confidence levels, implement repeatable outcomes and create audit trails and reports means that an automated solution is usually better able to manage, quantify and report on risks. From an internal compliance or regulatory perspective, this is a very good thing.

Designing a solution from the ground up which focuses on these types of issues will result in a much smoother path to market, and a more valuable solution once it is out there!

**GIVEN WHAT IS ACHIEVABLE TODAY, IT SHOULD BE RARE THAT A SOPHISTICATED AUTOMATED SOLUTION CANNOT MEET REGULATORY REQUIREMENTS.**

**THE REAL QUESTION IS: HOW DOES IT NEED TO OPERATE TO MEET THOSE REGULATORY REQUIREMENTS?**

## WHO IS LIABLE?

The short answer is, you are.

Well, at least if you are the one putting the solution to the market. If your customers are using it, then there is every chance you are liable for how it performs - or doesn't.

There are strategies to mitigate this liability contractually, but also operationally and in a technical or practical sense. The clearest example of this is how the auto industry is dipping its toes into autopilot for cars. The first step is "driver assist" – in layman's terms: "If you crash, don't blame us."

The beauty of this approach is not only that it helps overcome regulatory hurdles associated with fully automated cars and helps address the liability question, but it also enables the technology providers to get the product out in the real world sooner. This lets them collect more data and learn from every interaction.

Think about the stark difference between Google's data set on its driverless cars, which have driven 1.5 million miles in a closed development phase over the past few years, and Tesla's 100 million plus miles driven by customers using its Autopilot system. The Tesla cars log almost double Google's total miles every day.

When it comes to machine learning, data is key. This means that getting the product to market in a controlled manner - either through limited functionality or with a guidance/assistance model - is a huge advantage. This can get you to the next iteration faster than your competitors.

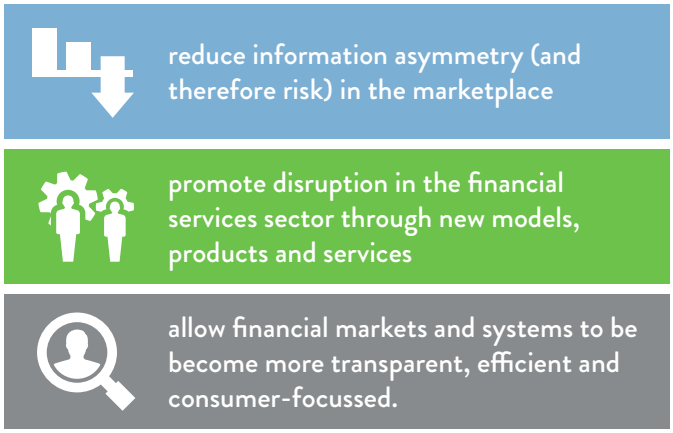
However, operational or technical approaches to mitigate liability aren't the full story. There is always likely to be some residual liability to be considered and your T&Cs need to carefully positioned to address this. Your marketing and promotional material also needs to be carefully considered so you don't sell a "driver assist" car at the same time as telling your customers "look, no hands"!

So, the first step is to find someone who gets both the technology and the law - and find them before you have built the thing! Only then will you get good advice on whether your new innovation is likely to run in to regulatory hurdles and how it can developed to operate in a compliant manner.

# FINTECH DATA MONETISED AND MONEY DIGITISED

PETER REEVES, SPECIAL COUNSEL, CORPORATE ADVISORY

## FINANCIAL TECHNOLOGY, OR "FINTECH" IS AN EMERGING GLOBAL FINANCIAL SECTOR USING TECHNOLOGICAL INNOVATION TO:




It has been described as "data monetised and money digitised".

Fintech is subject to extensive regulation covering registration, licensing and disclosure requirements; competence, capacity and conduct obligations; prudential standards; consumer protection (on multiple fronts); anti-money laundering counter-terrorism; privacy.....and the list goes on.

In Australia, fintech is seen as a focal point for economic growth. It is accepted that policy and reform in the financial services sector will be driven by fintech innovations. This has helped progress traditional thinking about how regulators apply the existing legal framework. Even so, the complexity of the legal and regulatory framework poses a test for fintech innovators.

The regime is administered by several regulators and navigating it is a challenge for a well-resourced and experienced player, let alone a start-up. For example, retail market place lending or fractionalised property investment platforms are often underpinned by collective investment structures and liquidity mechanisms - the registration and licensing requirements associated with these can be particularly challenging. To work through these successfully requires not only a solid understanding of the complex and onerous regulatory requirements, but also "out of the box" thinking in order to create a structures that fit into the existing legal framework. This in turn requires a willingness to challenge the traditional, comfortable thinking around how the framework has typically been applied and the ability to demonstrate that the necessary regulatory outcomes are being achieved through new models.

The Australian government and regulators have generally been responsive to these challenges. For example, ASIC is exploring a proposed "regulatory sandbox". This is intended to provide greater clarity about the skills and experience required by new businesses to be granted an Australian financial services licence, additional flexibility around demonstrating "organisational competence" in relation to restricted authorisations and a "regulatory sandbox exemption" enabling new businesses to run early-stage tests and trials.

The proposed regulatory sandbox includes a testing window, which:

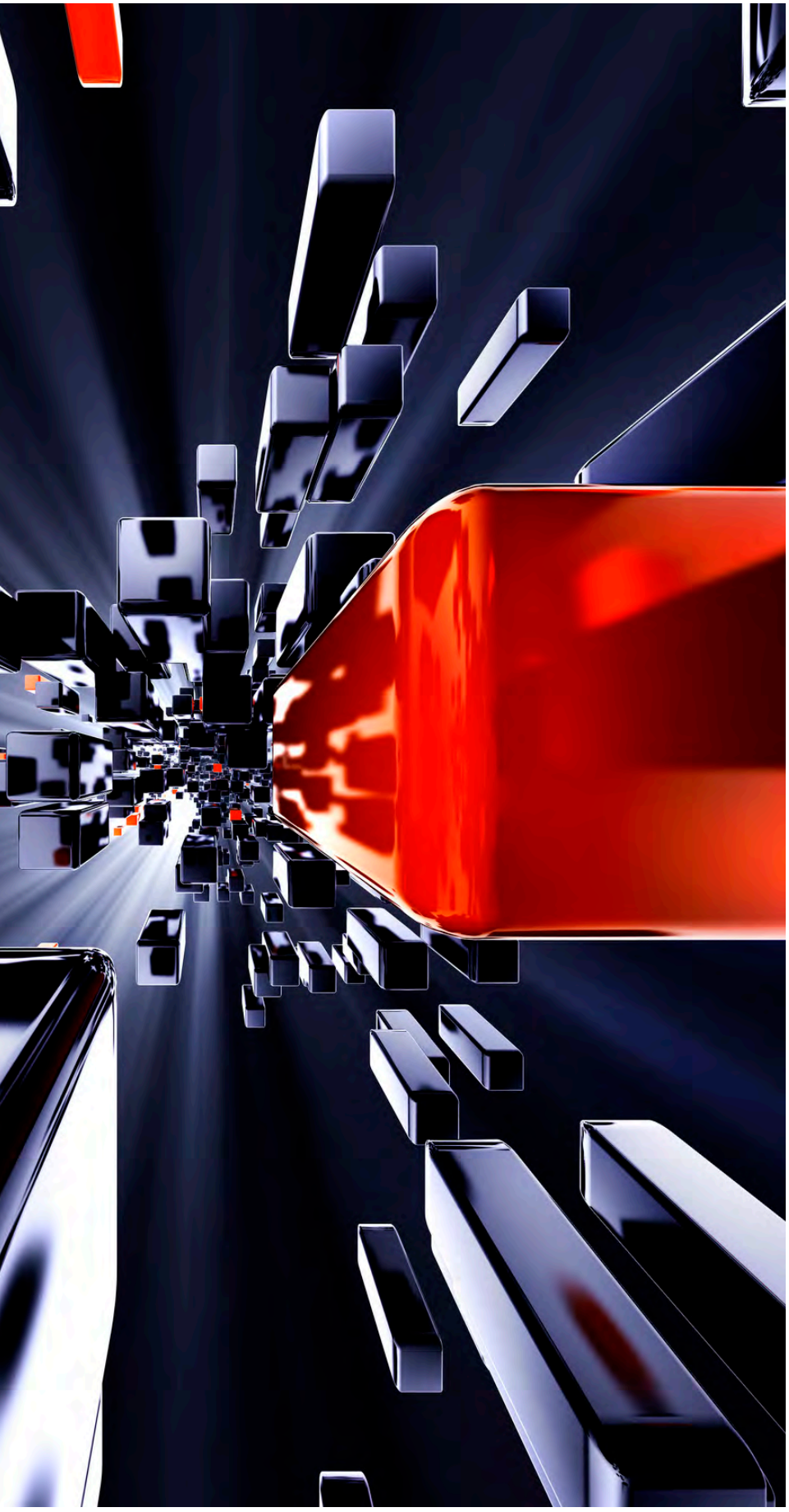
+ allows certain financial services and products to be provided without a licence
+ enables for sophisticated investors to participate with a limited number of retail clients with separate monetary exposure limits
+ modified consumer protections (external dispute resolution and compensation arrangements would typically apply in the retail environment) and
+ modified conduct and disclosure obligations.

The regulatory sand box exemption will be an important tool for early stage fintech as it addresses some of the key regulatory challenges for the industry.

# BLOCKCHAIN AND SMART CONTRACTS DIGITAL UTOPIA VERSUS THE REAL WORLD

BERNADETTE JEW, PARTNER, TECHNOLOGY, MEDIA + TELECOMMUNICATIONS AND PETER REEVES, SPECIAL COUNSEL, CORPORATE ADVISORY

**BLOCKCHAIN AND SMART CONTRACTS HAVE SET US ON A COLLISION PATH, POSING CHALLENGES THAT WE HAVEN'T HAD TO DEAL WITH BEFORE. PEOPLE WITH TECHNOLOGY, COMMERCIAL AND LEGAL EXPERTISE ALL NEED TO WORK TOGETHER IN THE BLOCKCHAIN ENVIRONMENT – AND THEIR EXPECTATIONS CAN BE QUITE DIFFERENT.**



- There are those who believe in a digital utopia, where everything can be converted into code. They believe that the digital world can solve the ambiguities and uncertainties of traditional legal frameworks.
- At its most extreme, this would require us to "live or die" by the code, regardless of the risk of coding errors. In fact, there are people who believe that the recent DAO incident (where coding errors were exploited to siphon away approximately US$50 million) was just a teething issue and that risks around coding errors will disappear over time.
- On the other hand, there are commercial operators who recognise that complexity, ambiguity and uncertainty are an inevitable part of commercial life (for better or worse).
- Just because you can code something, doesn't necessarily mean you should. There is always the question of whether the benefits stack up.

## A COLLISION PATH: TRANSPARENCY VERSUS CONFIDENTIALITY

We are seeing very real challenges in our day-to-day client work on blockchain around the collision between transparency and confidentiality.

Blockchain technologies are all about transparency – they were initially established for shared databases in which everyone sees what everyone else is doing. This transparency of the blockchain ledger is a key benefit. However, as we move from public to private blockchains, the goal is to leverage all the benefits of the blockchain environment while achieving required levels of commercial confidentiality. This is a complex area that is evolving both in terms of the technology solutions available and expert views about what is and is not suitable for the blockchain environment.

## SO, SMART CONTRACTS AND CONTRACTUAL AGREEMENTS: WHAT IS THE DIFFERENCE?

Without a smart contract, we couldn't exploit the full potential of the blockchain environment. Smart contracts are the computer programs that automatically execute processes affect changes on the blockchain ledger.

By comparison, a contractual agreement is about the intentions of the parties, and those intentions can be far broader in scope than just automated processing. The terms of contractual agreements can be manifest in many different ways: in writing, verbally, by conduct, by smart contract coding on the blockchain ledger – or by any combination of these.

## WHERE DO SMART CONTRACTS FIT INTO THE CONTRACTUAL AGREEMENT?

**Smart contracts provide the logic in the blockchain environment – with opportunities for far greater automation than we have ever seen before. However, smart contracts are not contractual agreements.**

Smart contracts are about more than just coding and automation of contractual terms. Smart contracts perform a role rather like that of a trusted third party - they will faithfully perform whatever tasks they are programmed to do in the blockchain environment.

A unique feature of the blockchain is its environment of "trust" which is achieved through consensus mechanisms and hashing algorithms. The participants on a blockchain ledger can validate every row in every record on the blockchain ledger without the need for a central validator. This makes the blockchain ledger tamper-proof – immune to risks of fraud and corruption. It also makes the blockchain ledger an ideal platform for the automated execution of contractual terms.

In this environment of trust, smart contracts are "self-executing" and "self-enforcing". Participants can trust the results of this automated processing. However, smart contracts don't replace contractual agreements. They only replace those parts of the arrangement that are suited to automated processing. This means that they are really no more than "smart transactions".

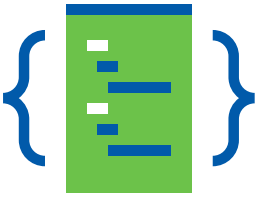
A contractual agreement can be far broader in scope than a smart contract. A contract may set out the intentions of the parties concerning things like rules for working together as a consortium on a private blockchain, managing decision-making around changes, handling coding errors and disputes. Many contract terms are not "deterministic" and can't easily be coded, although the scope of terms converted into pre-determined logic and code will expand over time.

## NEW APPROACHES TO CONTRACTING IN THE BLOCKCHAIN ENVIRONMENT

Contracting in the blockchain environment is not simply a matter of replacing traditional contracts with smart contracts. It requires a mix of smart contracts and contractual agreements as well as new approaches to address:

+ the practical challenges, risks, technologies and operational processes of the blockchain environment
+ the importance of facilitating ongoing change and agility in this fast-moving environment, and
+ the uncertainties and ambiguities of the commercial world, including specific requirements for more complex commercial arrangements on private blockchain platforms.

**SMART CONTRACTS PROVIDE THE LOGIC IN THE BLOCKCHAIN ENVIRONMENT – WITH OPPORTUNITIES FOR FAR GREATER AUTOMATION THAN WE HAVE EVER SEEN BEFORE. HOWEVER, SMART CONTRACTS ARE NOT CONTRACTUAL AGREEMENTS.**



# ACCC TOUCHPOINTS IN THE DIGITAL ECONOMY

CHARLES COOREY, PARTNER, COMPETITION + REGULATION

**RECOGNISING THE GROWTH AND IMPORTANCE OF THE DIGITAL ECONOMY IN AUSTRALIA, THE AUSTRALIAN COMPETITION AND CONSUMER COMMISSION (ACCC) HAS ESTABLISHED A SPECIALIST TEAM FOCUSSED ON "REGULATORY STRATEGY, DIGITAL ECONOMY & COORDINATION".**

This indicates that issues specific to the digital economy are squarely on the ACCC's radar, and its involvement in the digital economy is only set to increase. As Australia's leading competition law firm, we believe businesses need to be aware of the potential for the ACCC to take a strong interest in the digital economy and the most likely touchpoints for ACCC's activities to affect their operations.

## BIG DATA AND COMPETITION LAW

Access to data: Digital intermediaries (such as comparison websites, internet search engines and online marketplaces) collect vast amounts of data about the buyers and sellers on their platforms. Where big data analytics are applied and investments made to improve the quality of services, network effects may be amplified and barriers to entry heightened. This creates the potential to lock-out prospective competitors lacking access to data of equivalent scope or quality. Third parties who seek and are refused access to this data may allege that the data holder has misused its market power. Similar allegations have already been made by parties in the US and Europe. With an "effects test" to be introduced to the legislation shortly, risks to data holders will increase as it will no longer be necessary for an access seeker to prove that the data holder had an anti-competitive purpose. Instead, it will be enough to prove that the refusal to grant access to the data would have the effect of substantially lessening competition in a market.

Data exclusivity: The increasing number of data-driven business models emerging in sectors as diverse as the sharing economy, healthcare/diagnostics and transportation (via the Internet of Things) creates clear potential for ACCC intervention, in particular around contracts for exclusive data usage with third-party providers and tying data collected in one market to the sale of products or services in another.

Mergers & Acquisitions and dataset combination: The ACCC will be alive to the competition risks of mergers involving the combination of datasets. Unlike mergers in regular, non-data driven markets, the combination of a large incumbent and an innovative newcomer with access to a small but high-quality database may create concerns that the merger would have the effect of substantially lessening

**THE ACCC'S UNDERSTANDING OF THE DIGITAL ECONOMY AND INNOVATION IS INCREASING. HOWEVER, FOR THOSE AT THE FOREFRONT OF INNOVATION, IT IS WORTH ENGAGING WITH THE ACCC EARLY TO EDUCATE IT ABOUT YOUR NEW PRODUCT OR SERVICE.**

competition.

## A LEVEL PLAYING FIELD FOR ONLINE RETAILERS

In recent years the ACCC has received a significant number of complaints about manufacturers who:

- have denied online or mobile retailers:
- the right to sell the manufacturer's products on their platforms at all; or
- the same pricing terms offered to bricks and mortar retailers; or
- sought to prevent online retailers from reselling their products below a certain price.

As far back as 2011, Ticketek was fined $2.5 million for preventing 'Lasttix' from offering special discounted ticket deals. In 2013, in his annual "enforcement priorities" speech, Rod Sims from the ACCC dealt with this explicitly, saying "We will continue to give priority to online competition and consumer issues including conduct which may impede emerging competition between online traders or limit the ability of small businesses to effectively compete online."

Ensuring a level playing field for digital players is also a hot topic internationally. In July this year, the German competition law regulator took enforcement action against Lego for denying online retailers the same rebates that its bricks and mortar retailers were entitled to. Settlement was reached after Lego agreed to offer online retailers the same rebates.

## CONSUMER PROTECTION IN A DIGITAL WORLD

The emergence of the digital economy has seen the ACCC become increasingly concerned with:

- "drip pricing": the ACCC has described "drip pricing" as the "carefully constructed" online or mobile process under which a headline price is qualified and increased, bit by bit, until a final, higher price is arrived at. The ACCC is of the view that by the time the consumer reaches this stage in the booking process, they will reluctantly accept the higher price rather than go through the process again on the same or a different site. Following successful court proceedings against Jetstar and Virgin Australia, the ACCC has joined the International Consumer Protection and Enforcement Network's international sweep on drip pricing. Those in the travel and entertainment industries are especially in the spotlight;
- comparator websites: in 2015, the ACCC conducted a review of comparator websites and found that many involved exaggerated claims about the savings that consumers could make by switching to a alternate service provider. Outside of this study, the ACCC has a strong enforcement track record in this area: for example, in 2012, the online energy retailer comparison site 'Energy Watch' was ordered to pay almost $2 million for engaging in misleading advertising about the nature of its service;
- product review platforms and fake testimonials: online product reviews are now a key source of information for consumers. The ACCC has an ongoing concern that online review and testimonial platforms may be misused by business either through limiting negative reviews or by providing fake positive testimonials about a given product or service. The ACCC has taken action in the Federal Court against businesses posting fake testimonials and encourages online review platforms to prominently display any commercial relationship between the platform and the reviewed business;
- consumer guarantees and extended warranty representations: website operators also need to be aware of their obligations not to make false or misleading representations when it comes to the availability of the consumer guarantees provided for under the Australian Consumer Law. Where products suffer from a "major failure", consumers can choose between a refund, repair or replacement as well as receive compensation for reasonably foreseeable losses. This right exists regardless of any limitations a manufacturer's warranty or extended warranty may seek to impose. The ACCC has commenced a number of proceedings alleging contraventions in this regard. For example, in 2015, Fisher & Paykel and Domestic & General Services made a false or misleading representation in the course of offering an extended warranty to consumers, and were penalised $200,000 each.

## THE IMPORTANCE OF REGULATORY ENGAGEMENT IN THE DIGITAL ECONOMY

The ACCC's understanding of the digital economy and innovation is increasing. However, for those at the forefront of innovation, it is worth engaging with the ACCC early to educate it about your new product or service. The benefit of this can be avoiding a costly and distracting information request at a later stage stemming simply from a lack of understanding rather than from any material concern.

# CYBERSECURITY

BERNADETTE JEW, PARTNER,
TECHNOLOGY, MEDIA + TELECOMMUNICATIONS

**MANAGING ENTERPRISE RISK IN A DIGITAL WORLD POSES NEW CHALLENGES FOR CORPORATIONS, INCLUDING IN RELATION TO THE SECURITY OF CORPORATE DATA AND OTHER DIGITAL ASSETS; AND POTENTIAL DISRUPTION OF BUSINESS PROCESSES AND OPERATIONS, BOTH ONLINE AND ON-PREMISES**


These challenges are not just about cybersecurity and technical / compliance issues. The risks are multi-disciplinary – they overlap with business risks, supplier risks, responsibilities around reporting to the board, statutory disclosure obligations, litigation risks, reputational risks, corporate culture etc. They require an enterprise-wide approach – and best practice in the field is changing rapidly.

## A BALANCING ACT

No strategy can provide a 100% guarantee as to security – this is regardless of the size of the cybersecurity spend.

+ The amount of money wasted on specialised cybersecurity projects is alarming. The US Project Management Institute claims that only 56% of cybersecurity programs succeed in meeting their original purpose - and the impact to business is a loss of $109 million dollars on every billion invested in cybersecurity programs.[1]
+ The effectiveness of cybersecurity spend is reduced even further if a corporation allocates all of its spend to a particular area, and leaves itself exposed in other key areas.

Not all enterprise risks are created equal – managing these risks is a balancing act, and it requires a value judgment.

Whatever the available budget, corporations need to prioritise the risks, and "dial" the available budget so as to maximise its effectiveness across the corporation.

New approaches to governance are required – we need to manage the multiple dependences that impact on security of the enterprise, and we need to balance competing demands.

For example, there could be a technology approach which is going to enhance the security of the enterprise – but at the same time make it far more difficult for the technology team to manage and maintain the technical environment. These decisions can't be made within silos, they need to be weighed up on a whole-of-enterprise basis.

## DATA AS A STRATEGIC ASSET

Data is now a key driver of corporate efficiency and competitiveness. Cloud, mobility and the Internet of Things (IoT) are driving an exponential growth in corporate data - and data analytics is converting that data into a strategic corporate asset.

There are circumstances where corporate data may need to be treated as "sensitive data" – not just because of laws and regulations, but also where the data has commercial or strategic value or has potential impact on the corporation's reputation.

A best practice approach requires corporations to put their sensitive data front and centre - and it requires a much broader "data awareness" across the entire corporation.

## CHANGING THE WAY WE WORK

One of the fastest and cheapest means available to us in managing enterprise risk is to take a fresh approach to the way we work. It is no longer viable to just keep working in the same old way, and hope that the new risks of the digital world will look after themselves. We also can't assume that these risks are solely the responsibility of the technology or compliance teams. Every person in the corporation needs to play an active role in managing enterprise risk in a digital world – this is an essential part of creating a corporate-wide cybersecurity culture.

1 Project Management Institute, Pulse of the Profession: The High Cost of Low Performance (2014) page 4 <https://www.pmi.org/~/media/PDF/ Business-Solutions/PMI_Pulse_2014.ashx>

## HOW DO YOU DO MAKE THIS HAPPEN IN PRACTICE?

Traditional corporate silos get in the way – they result in people taking a narrow view of their areas of responsibility, and they allow risks to fall between the gaps. A change in culture is required - people need to be trained to understand that the management of enterprise risk (including cybersecurity) is their problem, and not someone else's:

**Step 1:** While most of us are not deep experts in security, technology or risk, we all need to understand the digital environment at a high level: (I) the corporate systems (II) the corporate data (including data transfers) and (III) the business processes - and how they all work together.

**Step 2:** Risk assessment needs to be approached on a holistic, end-to-end basis – and it starts with knowing the right questions to ask. Unfortunately, the "techy" language and concepts of the digital world often get in the way, and lead to communication gaps across the various corporate functions. We need to find ways of breaking down the language barriers, and working together with a common framework and taxonomy that embraces:

+ technical architecture and data structures, and controls
+ around access to networks, systems and data;
+ the complex world of security standards;
+ the broader framework of operational risk;
+ the commercial expertise of business and procurement teams; and
+ legal, regulatory and compliance expertise.
+ This framework also needs to extend to the corporation's third party suppliers, recognising their potential impact on the enterprise risk.

**Step 3:** We need to change the way that we work, and embed data-centric security processes into our day-to-day roles.

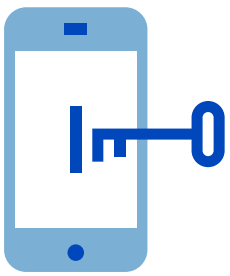
This requires a grassroots change. By way of example, it may require that commercial teams take an entirely fresh approach to procurement processes:

+ Procuring a new technology solution is no longer just about buying technology and delivering business outcomes. It also requires close scrutiny of the security consequences arising from that new solution.
+ As part of the procurement process, commercial teams need to have clarity around the sensitive data that will be created, collected, controlled, processed and/or transferred by any technology solution. And how access to that sensitive data will be controlled, logged and monitored?

We shouldn't assume or expect that corporate personnel will automatically have all of the skills required to make this happen in practice. These are new challenges, and no-one has the "been there, done that" skills. It is going to require a concerted program of "up-skilling", together with the rollout of new tools that will assist people to succeed in:

+ driving changes on the ground in relation to day-to-day practices and processes; and
+ communicating, co-ordinating and governing on a holistic basis in relation to the effective management of enterprise risk.

**THERE ARE ONLY TWO TYPES OF CORPORATIONS IN THE WORLD: THOSE THAT HAVE EXPERIENCED A CYBERSECURITY BREACH, AND THOSE THAT DON'T YET KNOW THAT THEY HAVE HAD ONE.**



# MAKING THE MOST OF YOUR DATA GETTING DATA ANALYTICS CONTRACTS RIGHT

PETER LEONARD, PARTNER,
TECHNOLOGY, MEDIA + TELECOMMUNICATIONS

## YOUR BUSINESS IS SEEKING TO EXTRACT VALUE FROM ITS NEWLY DISCOVERED TREASURE TROVE OF DATA. TO UNLOCK THIS VALUE YOU WILL OFTEN NEED TO WORK WITH OTHER PARTIES – DATA ANALYTICS SERVICE PROVIDERS AND CONTRIBUTORS OF OTHER, COMPLEMENTARY DATA SETS.

The problem is that many data analytics services contracts currently in use are not fit for purpose. Through our work with leading data providers and service providers in Australia, we have seen several common problems. We highlight below some key ways to get your contracts right – to unlock value and to protect your prized data assets.

### WHY ARE MANY DATA ANALYTICS SERVICES CONTRACTS NOT FIT FOR PURPOSE?

Big data analytics is a dynamic and rapidly evolving industry. Data analytics business models often change to reflect emerging technologies or shifting opportunities. We have found that many data analytics services contracts in common use are simple adaptations of data use agreements or software licence agreements. These contracts provide inadequate safeguards to the parties.

### TOO RIGID

These contracts often specify the expected outcomes from analytics services too rigidly and then are unable to deal with the inevitable pivots and changes that arise during the discovery phase of data analytics projects. They often lack effective ongoing governance mechanisms or transparent processes for re-pricing or realignment as these changes occur.

### INADEQUATE SAFEGUARDS

Data analytics services contracts should protect each party's valuable business information during the service term. They should also safeguard methodologies or insights arising from the project beyond the service term.

We believe that there are issues with many of the traditional safeguards used in standard data service agreements.

These include:

+ Copyright law concepts of 'who owns what' no longer work to effectively allocate ownership and rights of use. Australian copyright cases create significant hurdles to establishing ownership of databases or computer generated works – making it difficult to use copyright law to govern your data analytics projects.
+ We believe that a combination of targeted application of the law of confidential information (trade secrets), well-drafted contractual vertical and horizontal restraints and appropriate ring fencing arrangements can be effective to ensure fair and predictable allocation of rights. Poorly drafted contractual protections are often misunderstood or worse, simply unenforceable. If drafted incorrectly, vertical and horizontal restraints risk challenge under competition (antitrust) law, invalidity as unlawful fetters on employee mobility, unreasonable restraints of trade or impermissible extensions of intellectual property protection. Even where extensions of intellectual property are lawful in Australia, such extensions may not be enforceable in some jurisdictions, in particular in the USA. Fetters on employee mobility are also difficult to enforce in jurisdictions such as California and Germany.
+ Patents may not provide 'value for money' - other as comfort to venture capitalists or as defensive shields or 'tickets to trade' in the event of patent infringement claims by others. Your data analytics projects may rapidly evolve away from the originally anticipated processes and outcomes. As a result, patent claims often fail to provide patent owners with enduring freedom to operate

## PRIVACY: VALUE ENHANCING OR GETTING IN THE WAY?

We believe that a well-constructed privacy management process can be a significant value creator and source of competitive advantage in a data analytics deal. Unfortunately privacy regulation is seen by many businesses as addressing a problem – a compliance hurdle to be jumped rather than an enabler of a better deal. Privacy compliance is often addressed by simply layering more obligations onto the weaker party in the negotiation – a lawyers' version of 'pass the parcel'.

There is a better way. Well thought through privacy and information management creates optionality for future uses, reduces risk of later reworks, enhances the value of shared information and builds the trust of data partners, customers and regulators.

We work with clients to design end-to-end information management processes that are properly documented and verifiable. These processes consider privacy compliance in conjunction with protection of rights of use within the broader information lifecycle and service delivery chain. We address dependencies between a data provider and analytics partner and once information management mutually understood and fully transparent to each party. We then assist with appropriate allocation of responsibilities for effective de-identification of information and, where personal information must be used, provision of privacy notices and obtaining of consents.

**"THE DEFINITION OF 'PERSONAL INFORMATION' IN OUR PRIVACY LAWS DOES NOT EXPRESSLY DEAL WITH THE ISSUE OF DE-IDENTIFICATION."**

Anonymisation of transaction data and de-identification of personal information is crucial one to get right. If you can achieve reliable and verifiable de-identification (so that no individual can be re-identified by any recipient of that information, including through matching with other knowledge or data sets available to that recipient) then information may be used and disclosed without restriction under general Australian privacy law.

The definition of 'personal information' in our privacy laws does not expressly deal with the issue of de-identification. The growing consensus is that that the test to be applied is whether it is reasonably practicable for an entity receiving de-identified data to be able to re-identify an individual. This will be judged by a range of factors which include not only reference to the information itself, but also a recipient's ability to access other information reasonably available to the receiving entity.

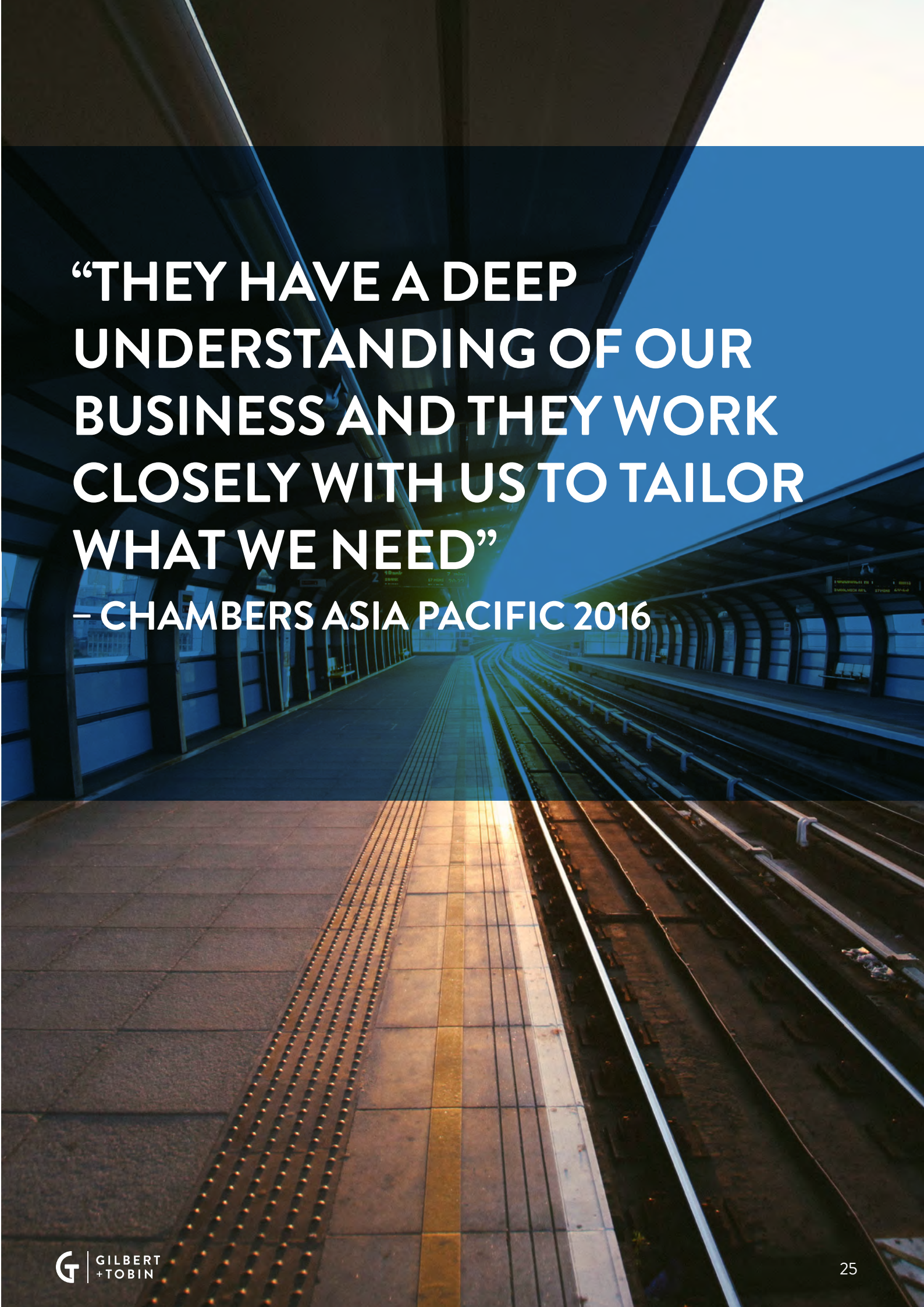
The risk of re-identification of any individual need not be completely eliminated, but it must be mitigated until it is (at least) low or remote. If you are sharing de-identified information you need to 'stand in the shoes' of possible recipients and then satisfy yourself before you release the de-identified information that the possibility of re-identification of any individual by the first recipient or any other reasonably anticipated downstream recipient is (at least) low or remote. In making this judgment, you may take into account reliable and verifiable risk mitigation controls and safeguards, technical (i.e. encryption, information security etc.), operational (clean teams, full data segregation and controlled access, etc.) and contractual. But you need to consider both the first recipient, upon whom these controls and safeguards may be contractually imposed, and any possible recipient further downstream. It's not what people say they will or won't do: it is what you fairly judge they cannot reasonably do. This judgement can't be fudged: it must be fair, expert and fully defensible.

## NEGOTIATING FIT-FOR-PURPOSE DATA ANALYTICS SERVICES CONTRACTS

To deliver value and strong protections in your data analytics services contracts, you should consider:

+ how to get an agile contract in place with appropriate (and at least adequate) protections, without 'boiling the ocean';
+ allocating rights in order to address shortcomings in copyright, patent and trade secret law;
+ ensuring that processes and data uses by each data partner are specified and well understood and protect against the leakage of value, such as through:
  - permitting additional commercially valuable uses that were not anticipated and therefore not factored into pricing and value calculations; or
  - – your competitors getting access to commercially valuable business information directly or indirectly through analysis of the data received;
+ drafting vertical and horizontal restraints that are fair and workable and also do not contravene competition laws;
+ facilitating clean disengagement on termination or expiry of the agreement, with each party able to re-engage with other data partners, including competitors, but with clarity as to subsequent uses and applications of project inputs, outputs, methodologies and processes and other learnings;
+ ensuring continuing alignment of upstream privacy statements and terms with downstream uses and disclosures (for compliance with privacy regulation);
+ not creating exposure to misleading or deceptive conduct claims that often arise, e.g. out of overly broad statements (for example, as to how 'any information that we collect about you' is to be used) or through unfair contract terms or through inadequate notice (such as vague statements about uses of de-identified information that are buried in privacy statements which purportedly only address uses of personal information);
+ anticipating and addressing fears and expectations of 'privacy advocates' and some consumers (including non-digital native consumers that may have greater sensitivities as to 'spooky stuff') and accordingly mitigating any risk that consumer trust and brand equity is undermined;
+ not being 'blind-sided' by collateral legal obligations including restrictions upon unlawful surveillance or use of tracking devices; fiduciary obligations; banker's and insurer's duty of confidentiality; potential availability of information collected under subpoenas or to regulatory authorities such as environmental protection authorities or to taxation or other government agencies; contravening restrictions upon discrimination that may be triggered by targeted offerings to segments of consumers and so on;
+ anticipating and allocating 'knowledge based liability risk' (i.e. exposure to negligence claims arising from failure to manage and/or mitigate risks based upon available information);
+ building in a 'big red button' to allow each party to appropriately address unanticipated major legal or reputational exposure without inadvertently creating an open backdoor of termination for convenience;
+ addressing possible future regulated access to ensure open availability or interoperability, as the focus of competition regulation shifts from the network layer to the applications layer or data layer.

Achieving good information management and negotiating fair and balanced data analytics deals is not easy. And that is why transparency of rights and use and good information management will be a key differentiator of industry leading data analytics businesses of the future. Corner-cutting or slapdash operators will wither away either through regulator action or mistrust of business partners. The stakes are too high to not do data analytics deals and information management really well.



# "THEY HAVE A DEEP UNDERSTANDING OF OUR BUSINESS AND THEY WORK CLOSELY WITH US TO TAILOR WHAT WE NEED"

– CHAMBERS ASIA PACIFIC 2016

# INNOVATION IS IN OUR DNA

## STRATEGY FOR BUSINESS AND LEGAL TRANSFORMATION

Gilbert + Tobin's Legal Transformation Team drive better business with:

### IN-HOUSE PATENTED LEGAL TECHNOLOGY

Gilbert + Tobin's dedicated in-house innovation hub collaborates with clients to develop bespoke technology solutions for workflow optimisation.

### ROBUST METHODOLOGIES

We apply a deep understanding of project management and process design methodologies to identify and implement fit-for-purpose business process solutions

### DATA-DRIVEN ANALYSIS AND INSIGHTS

We engage leading data scientists to drive data-led analysis across our clients' markets of interest, identifying trends and projections that enable better commercial strategies.

### LEVERAGING KNOWLEDGE

Gilbert + Tobin recently partnered with Westpac's Legal and Secretariat team and LegalVision, for an intense 24-hour design and coding event.

More than 50 lawyers and technology specialists delivered working prototypes to assist Westpac's internal legal team to deal with reoccurring and often time-consuming requests in an efficient and effective manner. Several of these prototypes are now being refined for implementation.


### INVESTING IN TECHNOLOGY DISRUPTORS

Gilbert + Tobin has invested nearly 20% in the virtual start-up law firm LegalVision - which is continuing to capitalise on growth and successfully take business from small and mid-sized firms.

Strategic move that allows us to service both ends of the market – from start-up to premium corporate brands.

Working on joint projects to develop legal applications for machine learning, artificial intelligence and blockchain in our respective markets.

Aligned with our passion for supporting the entrepreneurial spirit and fostering talent.

### RECOGNITION

#### INNOVATION IN USE OF TECHNOLOGY

Gilbert + Tobin recently won the award for Innovation in use of Technology at the Financial Times Innovative Lawyers Awards Asia-Pacific 2016 held in Hong Kong on 2 June 2016. This award was won for the legal hackathon Gilbert + Tobin hosted in conjunction with client Westpac and LegalVision in January 2016.

ESTABLISHED IN

# 1988

HAVE

## 70 PARTNERS

EMPLOYS OVER

# 500

**2016 ASIA-PACIFIC FT INNOVATIVE LAWYERS AWARDS**

Gilbert + Tobin was ranked third most innovative law firm overall in the Asia-Pacific headquartered category.

**"GILBERT + TOBIN'S TEAM IS ABLE TO 'INJECT STEP CHANGE IN THINKING FROM A COMMERCIAL AND STRATEGIC PERSPECTIVE."**

LEGAL 500, 2016

# G+T FULL SERVICE OFFERING

- BANKING + INFRASTRUCTURE
- COMPETITION + REGULATION
- CORPORATE ADVISORY
- CYBER SECURITY
- DATA, CONTENT AND PRIVACY
- EMPLOYMENT
- ENERGY + RESOURCES
- INTELLECTUAL PROPERTY
- LITIGATION + DISPUTE RESOLUTION
- REAL ESTATE + PROJECTS
- TMT
- TAX
- VIRTUAL DIGITAL


DANNY GILBERT

Managing Partner

Sydney

T +61 2 9263 4001

E dgilbert@gtlaw.com.au



SIMON BURNS

Partner, Technology
Media + Telecommunications
Sydney

T +61 2 9263 4776

E sburns@gtlaw.com.au



MICHAEL CAPLAN

Partner, Technology
Media + Telecommunications
Melbourne

T +61 3 8656 3333

E mcaplan@gtlaw.com.au



CHARLES COOREY

Partner,
Competition + Regulation
Sydney

T +61 2 9263 4019

E ccoorey@gtlaw.com.au



PAULA GILARDONI

Partner,
Competition + Regulation
Sydney

T +61 2 9263 4187

E pgilardoni@gtlaw.com.au



BERNADETTE JEW

Partner, Technology
Media + Telecommunications
Sydney

T +61 2 9263 4032

E bjew@gtlaw.com.au



JOHN LEE

Partner,
Intellectual Property
Sydney

T +61 2 9263 4776

E jlee@gtlaw.com.au



PETER LEONARD

Partner, Technology
Media + Telecommunications
Sydney

T +61 2 9263 4003

E pleonard@gtlaw.com.au



PETER REEVES

Special Counsel,
Corporate Advisory
Sydney

T +61 2 9263 4290

E preeves@gtlaw.com.au



PETER WATERS

Partner,
Competition + Regulation
Sydney

T +61 2 9263 4233

E pwaters@gtlaw.com.au



MICHAEL WILLIAMS

Partner,
Intellectual Property
Sydney

T +61 2 9263 4271

E mwilliams@gtlaw.com.au



MARSHALL MCKENNA

Partner,
Litigation
Perth

T +61 8 9413 8410

E mmckenna@gtlaw.com.au



PETRA STIRLING

Head of Legal Transformation

Sydney

T +61 2 9263 4750

E pstirling@gtlaw.com.au


GILBERT +TOBIN


**SYDNEY**

Level 35 International Towers Sydney
200 Barangaroo Avenue
Barangaroo NSW 2000
Australia
T +61 2 9263 4000
F +61 2 9263 4111

**MELBOURNE**

Level 22
101 Collins Street
Melbourne VIC 3000
Australia
T +61 3 8656 3300
F +61 3 8656 3400

**PERTH**

1202 Hay Street
West Perth WA 6005
Australia

T +61 8 9413 8400
F +61 8 9413 8444


**WWW.GTLAW.COM.AU**