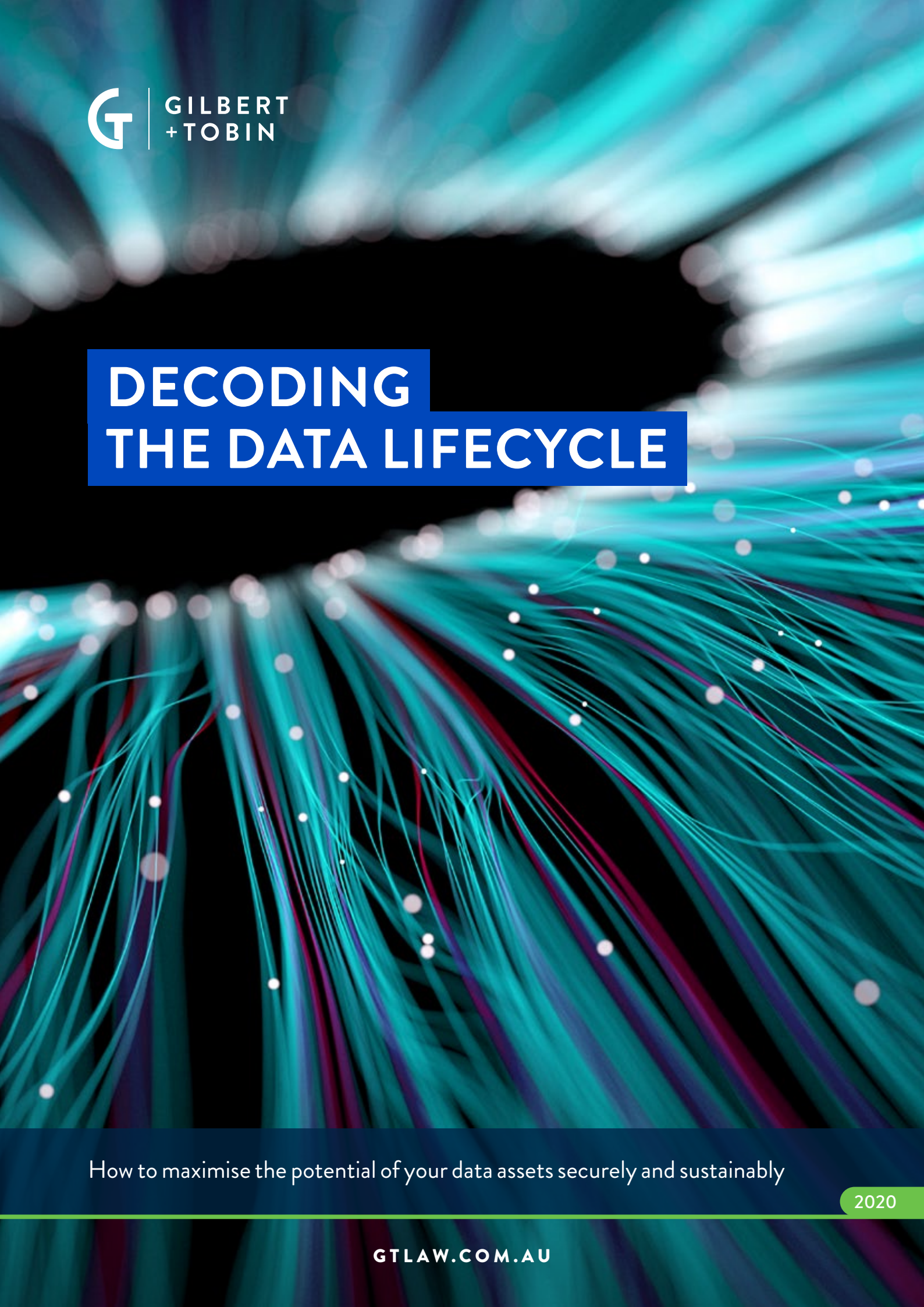


GILBERT +TOBIN

DECODING THE DATA LIFECYCLE

How to maximise the potential of your data assets securely and sustainably

2020

GTLAW.COM.AU

DEMYSTIFYING DATA

Given the relentless contemporary business, regulatory and media scrutiny on the subject, it is sometimes easy to forget that data isn't a new invention. To adopt and adapt the old cliché: data is both the new oil and the old oil.

Data has always been a valuable commodity in modern society. Controlling and manipulating datasets has long been a cornerstone of political power – census data, tax records and voting trends testify to this.

Businesses too have for time immemorial been custodians of large amounts of valuable data. However, until relatively recently (with a few notable exceptions) businesses have trailed far behind governments and civil society in using and capitalising on their data.

Too often, data was at best seen by businesses as a liability rather than an asset, and therefore something to be carefully managed by the technology team rather than the c-suite. Instead of seeking to derive value from their datasets, businesses have been pre-occupied with minimising their exposure to the regulatory and legal consequences of misusing data.

Until recently, this conservative approach wasn't necessarily a barrier to success. A cursory glance at a list of the top five largest companies by market capitalisation in 1980 demonstrates this clearly (IBM's millions were made through its hardware offering).

But fast-forward 40 years and the world has been turned upside down. We now live in an undeniably data-dependent age, where more data was generated in the last two years than over the entire course of human history, and where every person on earth now generates 1.7MB of data, **per second**.

And finally, the business world has taken note. A combination of rapid technological advancements and changing customer preferences has meant that the opportunities attaching to intelligent data use are now vast. In parallel, the consequences of poor data practices are equally huge, both from a loss of opportunity and a liability perspective.

It has become a cliché in recent times to note that data has been promoted to a seat at the Board table. The reasons for this are obvious – an equivalent list of top five companies today places data-centric businesses firmly front-and-centre of the modern economy (even Berkshire Hathaway invests heavily in technology companies, despite not being one).

At a more relatable level, over 90 per cent of Fortune 1000 companies are increasing their investment in data analytics and related technology.

In this context, businesses can't afford to be left behind – today's Netflix can become tomorrow's Blockbuster without the right focus and investment in company data assets. A deep understanding of your business' data journey, from generation to divestment or commercialisation, is a key part of achieving success.

To assist businesses and their advisors to navigate this initially intimidating and complex topic, we have sought to simplify the data journey by reference to a "data lifecycle". This breaks a typical company's data journey into digestible and discrete "stages", each of which comes with its own set of key considerations. Whilst the lifecycle is a simplification, it aims to provide you with the basic tools and arm you with the essential questions to maximise your data strategy.

Importantly, the lifecycle focusses on "value" not "risk". This approach seeks to empower businesses to maximise the potential of their data assets in a secure and sustainable manner. It is also worth noting that the lifecycle is not limited to personal data – it applies to all categories of data assets that a business may hold.

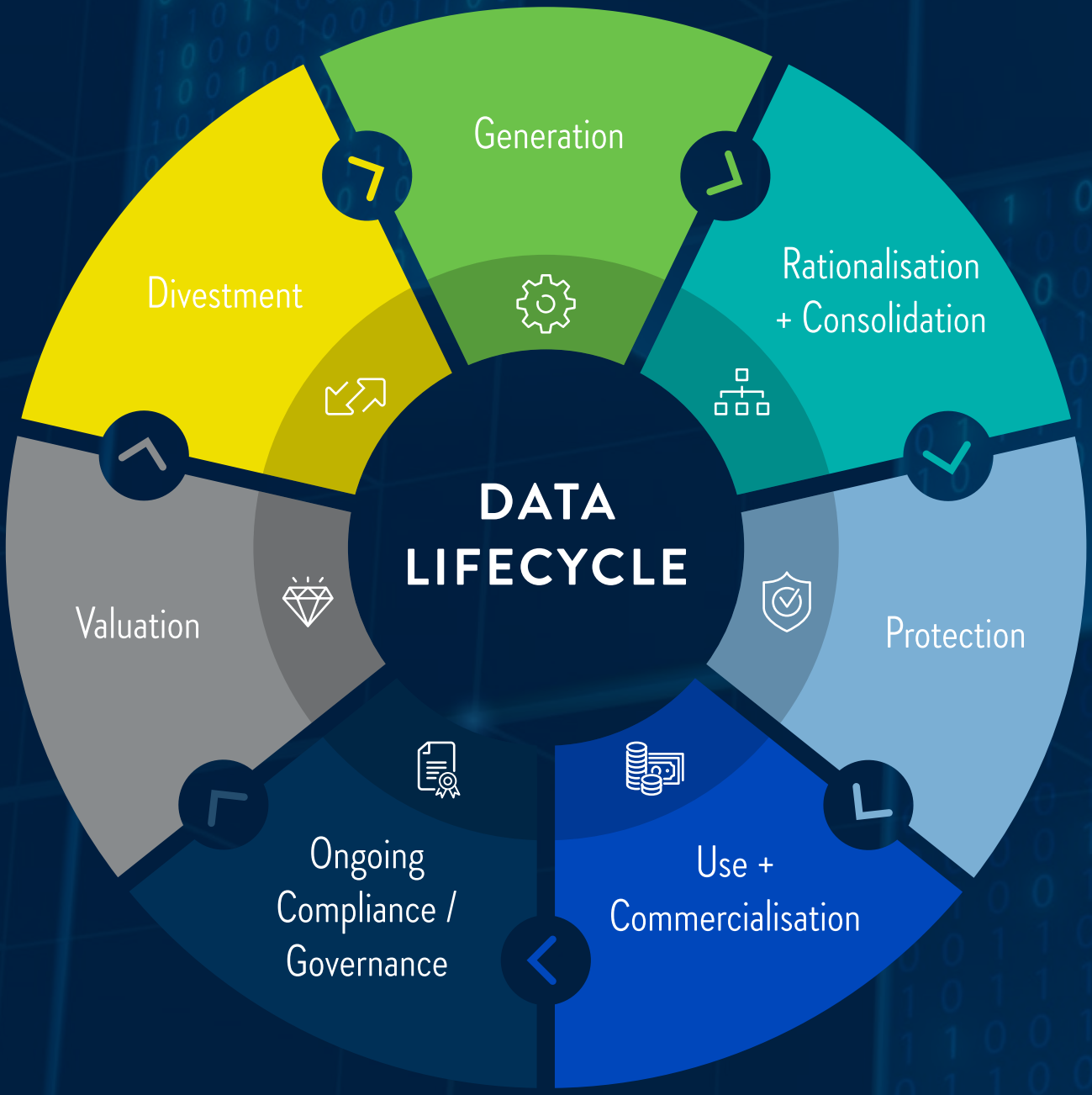
TOP 5 COMPANIES
THEN AND NOW

1980
IBM, AT&T, STANDARD OIL OF INDIANA, EXXON, SCHLUMBERGER

2020
APPLE, ALPHABET, MICROSOFT, AMAZON, BERKSHIRE HATHAWAY

"THE IT REVOLUTION IS EVIDENT ALL AROUND US, BUT THE EMPHASIS HAS MOSTLY BEEN ON THE T, THE TECHNOLOGY. IT IS TIME TO RECAST OUR GAZE TO FOCUS ON THE I, THE INFORMATION."

Viktor Mayer-Schönberger


DATA LIFECYCLE
Generation
Rationalisation + Consolidation
Protection
Use + Commercialisation
Ongoing Compliance / Governance
Valuation
Divestment

GENERATION

A business can generate data in several ways, including by acquiring data from external sources, modifying existing datasets, or collecting data as a part of its business activities. Given the potential breadth of these activities and therefore how fundamental the generation of data is to carrying on a business in the 21st Century, it is important to think of every business as a data-generating business.

Data itself can come in various forms and guises and from a wide range of (sometimes unexpected) sources, including from website traffic, social media platforms, customer communications, the processing of orders / sales and the acceptance of payments. Whilst some businesses will generate primarily personal data, others may generate swathes of machine data.

Regardless of the nature of the data involved, generation is the critical first step on a business' data journey and getting this right will ultimately dictate how successfully a business is able to use and commercialise its data down the line. Things to think about at this early stage include:

+ the development of a **clear corporate strategy** and business evolution plan for data. Having a clear strategy from the get go will allow a business to unlock opportunities at later stages of the lifecycle, including for when a business is seeking to rationalise, use and commercialise the data it has generated.
+ the **terms of collection and acquisition** that will attach to the data a business generates. How will those terms capture (or restrict) the full range of potential uses contemplated for that data?
+ if data is to be collected from data subjects, how will **full and informed consent** be obtained from those data subjects? This is key to ensuring that the data can be fully utilised down the track, including for purposes that may not have been known up front (noting that this issue is currently front of mind for regulators such as the Australian Competition and Consumer Commission (**ACCC**)) and may involve consumer law and privacy law considerations. Additionally, some foreign jurisdictions have more onerous expectations when it comes to data generation and consent, such as the EU's GDPR.
+ **steps that should be taken to protect data from the outset**. For example, it may be best to opt for proprietary and confidential data where possible (rather than taking data from public or third-party sources) and consider any surrounding intellectual property (**IP**) rights, such as those in software (or possibly databases).
+ how can any **IP infringement risks be mitigated**? IP considerations may impede commercialisation down the track, for example if there are any third-party claims. It will be important to deal with any **ownership rights** up front if there are multiple parties involved.
+ given a business may ultimately want to commercialise the data it has generated, it should seek to **understand the financial value** of any data generated throughout its lifecycle (see: valuation).

RATIONALISATION + CONSOLIDATION

Once a business has generated its data, it must turn that data into something useful. The volume of the data that any business holds is secondary to its ability to derive meaningful information from it and this is where rationalisation comes in.

Rationalisation of data can be achieved through traditional (technology-enabled) data-structuring methods, or more informally through business leaders and subject-matter experts deciding which types of data are or are not critical to their strategy. Some points to bear in mind:

+ rationalisation will not only allow a business to have better visibility over a data set, but can **lead to better outcomes throughout the data lifecycle**, including more focussed decision making, more resource-efficient approaches to storage and protection, and improved opportunities for commercialisation.
+ altering the attributes of the data may allow a business to achieve the **same desired results, with less regulatory burden**. For example, anonymisation or pseudonymisation of personal data may enable a business to meet its data protection and privacy obligations whilst still gaining useful insights.
+ when it comes to employees effectively leveraging data, accommodating data is only half the battle. Ensuring an **appropriate method of data search and access** is available to employees will increase the value in any business' data.
+ rationalisation **may increase the prospects of copyright protection attaching to data**, depending on the type of data and how it's organised. Having said this, copyright protection requirements for human involvement in the process of rationalisation may not sit well with many automated approaches to data organisation today.
+ note that any **sector-specific regulations** concerning data integrity and restricted data alteration may limit the ways in which certain types of data can be rationalised.

> **"THEY ARE VERY COMMERCIAL AND GOOD AT FINDING WAYS TO MAKE THINGS HAPPEN."**
>
> Chambers & Partners Asia-Pacific

PROTECTION

Once a business has rationalised and consolidated its data, that data becomes increasingly useful and may reveal commercially valuable information or detailed insights about customers or key business processes (including perhaps the personal or sensitive information of data subjects).

Utility, however, is a double-edged sword. What is useful to a business will also be useful to others and what is valuable to a business and to its stakeholders will be a prime target for anyone seeking to undermine that business.

As a result, a business not only has legal and regulatory obligations to adequately protect the data that it holds but is also subject to overwhelming commercial imperatives (including from a reputational perspective) to protect that data. Some key steps may include:

CYBER AND INFORMATION SECURITY

Implementing appropriate cyber and information security processes from both technical and operational perspectives to prevent against data breaches.

TERMS OF DISCLOSURE

If a business is disclosing data to any service providers or other third parties, it will need to consider the contractual models it has in place with these parties, including whether any terms of disclosure impose adequate restrictions.

COPYRIGHT PROTECTION

Considering whether copyright protection is a possible avenue for protection of data (although, increasingly copyright is becoming the exception rather than the norm for large data sets).

PROTECTION STRATEGY PLAN

Developing a protection strategy plan. A business should ask: to what extent do its legal protections, operational protections (such as technological and security measures) and cultural protections (such as messaging, training and leadership) play a part in this strategy? At a basic (but critical) level, what low-tech, day-to-day measures can be implemented? For example, developing procedures around communicating information on a need-to-know basis, using password protection for documentation and promoting good internal cyber practices.

CONFIDENTIAL INFORMATION AND CONTRACT LAW

If a business is deriving insights or correlations from big data sets, laws protecting confidentiality and contract law are key tools for protection.

USE + COMMERCIALISATION

All roads on a business' data journey should lead towards manufacturing the optimal use and commercialisation of its data assets. There are innumerable ways to derive value from data, from extracting insights from a data set to create commercial opportunities, to the sale or licensing of data assets. Subject to varying regulatory obligations and constraints, businesses around the world are exploring creative approaches to data commercialisation.

A business should consider carefully **the best way for specific data sets to be commercialised**. For example, the complete sale of data may be less advantageous for various reasons, including restricting a seller from using that data going forward. An alternative might be to license that data, in which case the business will need to think about the basis on which licensing should occur, for how long, and for what purposes the licensee can use the data.

When licensing data, it can be difficult to carve up intangible assets over different territories. One of the main challenges will be the **treatment of new data or IP** that stems from the use of licensed IP. It will also be relevant to consider what protections the licensee should be required to have in place when using the licensed data.

Data commercialisation can be a **great source of competitive advantage** and can often draw from existing (though latent) data assets generated by your business. Analysis of these assets can reveal the need for new market offerings or customer approaches or locate areas to boost internal operational efficiency.

Data trusts are an emerging area of data commercialisation. Not trusts in a legal sense, data trusts are bespoke contractual and corporate models designed to introduce transparency and structure to data sharing. In commercial settings, they respond to the need to derive value from data while still maintaining stakeholder trust and legal compliance.

The extent to which data can (or should) be commercialised also involves **ethical considerations**. It may not necessarily be a question of "can we?" but "should we?" A business may ask itself: was the source of the data aware of our commercial intentions at the time of collection? Is our analysis accounting for the impact of any underlying bias in the data set?

ONGOING COMPLIANCE / GOVERNANCE

Depending on the type of data a business holds and the sector it operates in, regulatory compliance and information governance may need to be front-and-centre of a business' approach to data management. In 2020, the regulatory landscape governing data is far more complex than in times past and extends beyond traditional privacy and information security considerations. To add to this complexity, this landscape is far from settled. The following areas may influence a business' ongoing compliance and governance practices.

+ **Competition law** is catching up with a data-driven business world. Increasingly regulators are recognising that data can be a source of market power and are expressing reservations about combinations of data sets (or data businesses) on the basis that these combinations may have a significant impact on a market (or across markets) and consumers.
+ **Privacy law** is also developing to enhance consumer awareness and control, especially regarding ongoing, real-time consents. It is important to consider that regulatory compliance may also extend beyond a business' 'home' jurisdiction, with the proliferation of extraterritorial laws overseas, such as the GDPR and California Consumer Privacy Act.
+ **Consumer protection law** in Australia is evolving to take greater account of the concealed data practices of businesses. For example, the **Digital Platforms Inquiry** (**DPI**) recommended that the current unfair contract terms regime ought to be revised to better take account of how data businesses can uniquely undermine consumer interests.
+ Australia recently established a **Consumer Data Right** (**CDR**), increasing the portability of data and bolstering consumer choices. Whilst the CDR will only apply to the banking sector initially, it is set to extend to the energy and telco sectors in the future (and may expand to others).

> **"GILBERT + TOBIN ATTRACTS MANY OF THE MOST COMPLEX AND NOVEL IT PROJECTS FROM BOTH GOVERNMENT DEPARTMENTS AND CORPORATES AND IS HAILED FOR BEING 'ENGAGED AND CREATIVE'. "**
>
> Legal 500

VALUATION

Although we have placed the valuation stage towards the end of our data lifecycle, in practice valuation is an ongoing and iterative process that must take place throughout each stage of the lifecycle.

For example, understanding the value of prospective data assets is key to being able to invest sensibly in their generation. Additionally, a business must also have valued its data assets before it seeks to commercialise them, or before it can effectively and accurately report on how they form part of the overall assets and liabilities of that business (including in respect of any shareholder engagement or other regulatory requirements). And of course, valuation of data will play a central role in any divestment activity.

In each case, valuation activities will likely require engagement from external stakeholders, including accounting, tax and financial advisors.

There may be a number of factors which influence the value which may be ascribed to any data set, which may include:

How **data value may be offset or balanced against any risk** inherent in that data. Not all data is equal, for example, health data is very valuable, but it is also regulatorily burdensome.

Understanding what the data is and where the **opportunity** lies. Are there any untapped purposes for which the data can be used, and can those purposes be utilised and priced?

Considering which **method of valuation** will be most appropriate when taking account of the outputs from data commercialisation. For example, is there a market value for the data, or is it more appropriate to use a costs-based approach or consider income methods?

DIVESTMENT

The final stage of the data lifecycle focuses on circumstances where a business is seeking to divest the data it owns. This may form part of a broader share or asset sale of the data-rich business or may be a discrete divestment of the data assets only.

Given that every business is now a data business, regardless of the form the divestment takes, data is likely to be a key focus – with its own bespoke considerations. Our experience is that this focus is growing ever stronger, with data related matters and potential opportunities increasingly driving key decisions at the point of sale.

In each case, a business that has subscribed to a clear and well-developed data strategy (from generation to divestment) will increase the likelihood of success of any divestment it wishes to undertake. For example, having a clear understanding of the rights, protections and 'chain of title' of any data and its outputs since generation, will be essential to any transfer.

A divestment will require a business to consider a number of data-specific considerations, including for example:

PROPOSED USE OF THE DATA

An acquirer's proposed use of any personal data post completion, particularly if the nature of the business may be changing.

PRIVACY OBLIGATIONS

The privacy obligations imposed on the vendor and acquirer. Both parties will need to ensure they protect individual privacy rights throughout a transaction, disclosing personal information only where disclosure is necessary to assess the business.

LIABILITY POST SALE

Will the vendor have any liability post sale? What are the nature of any representations and warranties relating to data in the transfer documentation and what are the implications of these? A vendor should consider its ongoing liabilities in relation to different categories of data and provide for those appropriately in any transfer documentation.

WARRANTIES AND INDEMNITIES INSURANCE

Data is a focus area of warranties and indemnities insurance. Insurers often find it difficult to test data specific issues, such as the vulnerability of a business to cyber threats, opting instead to exclude data related coverage or provide stringent exceptions.

CROSS BORDER CONSIDERATIONS

Are there any cross border considerations? Vendors must know where their data is located and understand the implications of this if other jurisdictions are involved. Some jurisdictions may have different requirements for the transfer of different categories of data and this can impact how a transfer is structured or conducted.

FIRB

Where foreign acquirers are involved, the Foreign Investment Review Board (**FIRB**) may impose conditions on how any foreign entities may use, deal with and transfer any data they acquire.

TRANSITIONAL SERVICES

Will the vendor need to provide any transitional services to the acquirer post completion to allow the acquirer to derive value from the data? If so, how long for and on what terms?

ACCC

Whilst data can vary in competitive significance it is increasingly at the forefront of regulator minds such as the ACCC when assessing transactions. Transactions which may previously have raised no concerns are being viewed in new light as regulators seek to understand how the combination of distinct data sets may create new competition and market power issues. In Australia, the ACCC is viewing data as especially valuable in digital markets.

AUTHORS

SIMON BURNS
Partner
T +61 2 9263 4776
M +61 448 100 727
E sburns@gtlaw.com.au

MICHAEL CAPLAN
Partner
T +61 3 8656 3333
M +61 413 605 274
E mcaplan@gtlaw.com.au

MELISSA FAI
Partner
T +61 2 9263 4685
M +61 404 873 252
E mfai@gtlaw.com.au

TIM GOLE
Partner
T +61 2 9263 4077
M +61 410 540 745
E tgole@gtlaw.com.au

ANDREW HII
Partner
T +61 2 9263 4046
M +61 457 808 018
E ahii@gtlaw.com.au

SHEILA MCGREGOR
Partner
T +61 2 9263 4152
M +61 414 399 976
E smcgregor@gtlaw.com.au

LESLEY SUTTON
Partner
T +61 2 9263 4296
M +61 414 265 169
E lesutton@gtlaw.com.au

STEPHANIE ESSEY
Lawyer
T +61 2 9263 4034
M +61 407 011 248
E sessey@gtlaw.com.au

CHERRIE FUNG
Lawyer
T +61 2 9263 4727
M +61 410 539 646
E cfung@gtlaw.com.au

ILONA HUNNISETT
Lawyer
T +61 2 9263 4058
M +61 402 019 257
E ihunnisett@gtlaw.com.au

ANDREW LOW
Lawyer
T +61 2 9263 4793
M +61 414 509 421
E alow@gtlaw.com.au

NIKHIL SHAH
Consultant (Admitted in England Wales, not admitted in Australia)
T +61 2 9263 4048
M +61 477 100 990
E nshah@gtlaw.com.au

REBECCA SMITH
Lawyer
T +61 2 9263 4076
M +61 499 799 768
E rsmith@gtlaw.com.au

ANNA BELGIORNO-NETTIS
Lawyer
T +61 2 9263 4409
M +61 422 774 229
E abelgiorno-nettis@gtlaw.com.au

SOPHIE BOGARD
Lawyer
T +61 2 9263 4525
E sbogard@gtlaw.com.au

BRYCE CRAIG
Lawyer
T +61 2 9263 4555
E bcraig@gtlaw.com.au