Allens › ‹ Linklaters

Benefits over backlash

FIVE STEPS TO A FIT-FOR-PURPOSE DATA STRATEGY FOR GENERAL COUNSEL

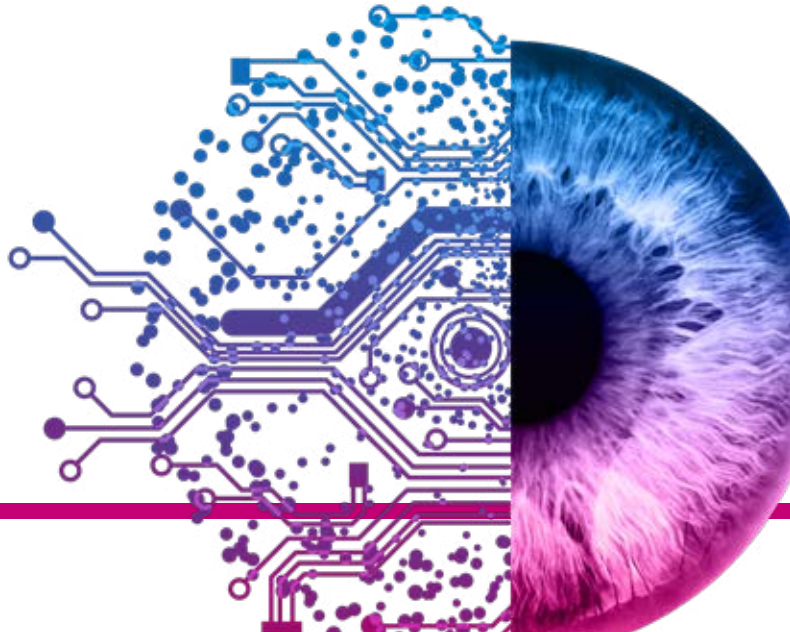
Recent data scandals and the consumer backlash against privacy intrusions call for data strategies that prioritise trust, transparency and consumer control. Our research shows many organisations are only at the beginning of this journey.

It's all too easy in the current environment of public mistrust for organisations to adopt a conservative approach to data exploitation. But the aims of leveraging data assets for benefit while maintaining consumer trust are not mutually exclusive. To achieve both, senior executive teams must deploy and endorse a holistic, robust data governance program across their organisations. They must uplift their consumer-facing engagement on data beyond bare legal compliance to a new level of transparency and trust creation.

GENERAL COUNSEL SHOULD ACT NOW TO EDUCATE SENIOR LEADERSHIP – BOTH AT THE EXECUTIVE AND BOARD LEVEL – AND TO BUILD AND IMPLEMENT THOSE DATA GOVERNANCE AND CONSUMER ENGAGEMENT STRUCTURES.

In the past 12 months we've seen a swing in the pendulum of public attitude towards the use of data by organisations. This is exemplified by the Ponemon Institute's stark finding that Facebook users' confidence has suffered a 66 per cent decline by comparison to the same survey in 2017 following the Cambridge Analytica scandal.[1] In Australia, that damage to consumer trust has seen a re-intensified campaign for individuals to opt out of the government's My Health Record scheme, on the basis that it might pose a risk to individual privacy.

We don't think this should lead organisations or governments to halt or slow down responsible data exploitation strategies. The business and societal benefits of enhanced data enrichment, analysis and liquidity are too great for that to occur. But organisations do need to invest time and money in creating new mechanisms to ensure their data programs are well-governed, transparent and operated through an ethical lens. Our research shows many organisations are still only at the beginning of this journey.



1 Facebook Privacy Trust Survey, Ponemon Institute, 2018. Most Trusted Companies for Privacy, Ponemon Institute, 2017.

Successful data strategy starts at the top

For a data strategy to create tangible and consistent impact throughout an organisation, it must first be implemented through a clear data governance program that is endorsed at the highest levels of the organisation.

Some organisations and sectors are already well advanced in this space. But many others are still building the knowledge base required to implement effective data governance.

ACCORDING TO OUR RESEARCH, APPROXIMATELY 70 PER CENT OF ASX 200 BOARDS DO NOT HAVE TECHNOLOGY AND DATA EXPERIENCE.[2]

This creates renewed importance for the role of legal counsel on organisation-wide data governance. In many cases it will be up to legal counsel to educate senior executives on robust, holistic data governance for their organisation.

To ensure consistency and widespread cultural adoption within organisations, a data strategy and its governance program must be owned and operated by the entire organisation. It is no longer possible to confine its stewardship to any one business unit.

Internal processes and mechanisms are only one side of the coin. The other side requires organisations to substantially re-think the way they create a trust compact with their customers by raising the bar on transparency and consumer control over data. Organisations can achieve a real point of differentiation in the market by doing so.

Legal counsel are uniquely placed to lead data strategy and to provide reasoned advice across multiple business functions. Here's how.

Almost half of ASX 200 privacy policies have **not been updated** in the past two years.[3]

1 Create consensus on principles for good data governance

An agreed set of data management principles is crucial

While data use was once narrow enough for data governance to specify instructions for each use case, the increasing scale of data use means this is no longer possible. Instead, successful data strategy relies on agreed principles deployed consistently at all levels of the organisation, from CEOs making decisions on third party data sharing to sales assistants entering customer details into databases. This ensures that practice remains consistent as new opportunities and innovative use cases arise. It also creates a structural balance between safeguarding against risk and exploiting potential rewards.

Where an organisation's philosophy on data use is unclear, in-house legal teams' are unable to collaborate swiftly with operational teams to enable opportunities and mitigate risk. This perpetuates a loop of reluctance to seek input from legal, and general confusion and inefficiency.

2 Allens research, 1 November 2018.
3 Allens research, 1 November 2018.

Be transparent to protect against risk

2 *Develop a comprehensive map of data use cases at your organisation – both current and future – and ensure these uses are made clear to customers in a simple and engaging manner*

A focus on mere compliance with privacy laws and the adoption of broad-based consents and generalised privacy policy disclosures runs the risk of leaving consumers disinterested or, worse, alienated. It should be immediately obvious to your customers what they are signing up for – how their data is collected, how it is used, when it might be shared with third parties, how it might be commercialised, how it is protected and when it will be retired. Provided data is being used ethically and securely, removing the knowledge gap between perceived and intended use will help to protect customer loyalty and safeguard against critical reputation issues.

A common view for many organisations has been that detailed, granular transparency in privacy policies and other communications about data use runs the risk of creating customer alarm as well as inflexibility for the organisation. There has also often been a preference to bury consents in the depths of impenetrable terms and conditions, which are in turn tied to overly generalised permissions about the use and sharing of data. The theory has been to adhere to the minimum level of legal compliance, believing that the less the consumer is specifically alerted about data use, the less likely they are to be outraged.

In reality, the opposite is now true. Consumers' outrage surrounding data use is most often sparked by a mismatch between their understanding and the organisation's actual practices, with those practices often obscured behind vague generalisations. This lack of clarity creates risks for consumer trust and, by extension, for meaningful and beneficial data use. Best practice data strategy calls for simple, transparent communication with customers. Single-screen, symbol-based communication should be used to ensure data labelling is as easily understood as laundry care instructions or country of origin labelling on food.

3 Empower your organisation to communicate value to consumers

Clearly communicate the benefits to consumers of sharing data

Meaningful communication of the value transaction taking place when data is shared is an essential counterweight for transparency. Consumers need to know how their data will be used, but also what they'll get in return. Forty-one per cent of Australian consumers are comfortable allowing a trusted brand to transfer their information to third parties if there are clear benefits to doing so.[4]

This creates the need for better collaboration across business functions, particularly between legal and marketing teams. There is sometimes a divide between legal and business operations teams in organisations where marketing teams, for example, may avoid liaising with legal teams because they fear their attempts at creating communication will be rejected. There is a positive role for lawyers to play here: lawyers can act as enablers, informed by the organisation's agreed data governance principles.

To foster both consumer trust and commercial success, organisations must offset transparency with value communication. In our experience, organisations that combine these two elements are most likely to best leverage their data assets successfully.

4 The Symbiotic Relationship Getting the balance right, Deloitte Australian Privacy Index, 2018.

4 Banish 'set and forget'

Regularly updating your organisation's policy and practices is important, but frequently forgotten

Our research found almost half of ASX 200 privacy policies have not been updated in the past two years. In fact, approximately 20 per cent of ASX 200 companies have not updated their privacy policies since 2014, when the most recent overhaul of privacy legislation took place. Four per cent don't have a publicly available privacy policy at all.

Clearly, this is out of step with the transformation in data use in recent years. It also provides a window into the disconnect between increasing sophistication of data use on the one hand and transparency inertia on the other.[5]

The scale and sophistication of data use has now reached a point that was unimaginable 10 years ago. Likewise, it's virtually impossible to predict what will happen in the next three to four years. This means data strategy must be constantly updated in step with new use cases, capabilities and regulatory changes.

The full spectrum of data use – including both strategy and privacy and security compliance – must be front of mind at any point where data is collected and used. Every element should also regularly be considered and audited afresh.

5 Protect your assets

Data strategy is worthless without best practice cybersecurity

As organisations continually find new and more innovative ways of working with data, cyber criminals are finding more sophisticated ways to access it. As the crown jewels of your organisation, the value of your data extends beyond your borders.

Put simply, there's no point investing in data if it's not secure. Your data will be worthless if it is already accessible in the market. More importantly, the erosion of trust with your customer base in the event of a breach could be fatal.

Like privacy, security needs to be implemented at every point where data is collected, used and commercialised. It also needs to constantly evolve in step with new technologies and use cases, preserving trust and protecting one of your most valuable assets.

But security mechanisms are not just about protection. They are also an enabler for enhanced data exchange, enrichment and analysis. That's why we advocate for the use of de-identification methodologies and secure platforms for undertaking data analysis and creating new insights. Deploying industry best practice de-identification techniques can be an important part of the overall trust package with consumers.

No turning back on data use

A relatively small number of high-profile issues or campaigners should not be allowed to derail the huge benefits that can be derived from data for organisations, consumers and society more broadly. But to achieve that, organisations must invest in sophisticated data governance programs, re-focus on the ethical use of data and overhaul their approach to transparency and consumer control. Used well, data can improve business operations, drive customer loyalty and add millions to balance sheets.

CONTACTS

Gavin Smith
Partner, Head of Technology, Media and Telecommunications
T +61 2 9230 4891
Gavin.Smith@allens.com.au

Valeska Bloch
Partner
T +61 2 9230 4030
Valeska.Bloch@allens.com.au

Michael Morris
Partner
T +61 7 3334 3279
Michael.Morris@allens.com.au

Michael Park
Partner
T +61 3 9613 8331
Michael.Park@allens.com.au

Ian McGill
Partner
T +61 2 9230 4893
Ian.McGill@allens.com.au

allens.com.au/data*driven*business

5 Allens research, 1 November 2018.