THE EVOLVING WORLD OF PRIVACY COMPLIANCE

Strategies for managing data governance and cyber risk to meet legal and regulatory obligations

Published March 2023

Contributors

BigID

Intalock
Powered by Spirit

LANDER & ROGERS

Contents

Abstract

In the Fourth Industrial Revolution, our fascination with information and data knows no bounds. Organisations are under increasing pressure to leverage data as part of their corporate strategy. But, at the same time, demands on data have never been more conflicted. On one hand, data provides insights that can unlock new opportunities or efficiencies, and on the other it exposes organisations to increased governance-related risks.

In an environment of wide-reaching privacy law changes, heightened regulatory oversight and scrutiny, and ever-evolving cyber threats, effective data management and governance are now non-negotiable.

This white paper proposes an enterprise-wide solution that brings a cross-disciplinary approach to data and privacy management to optimise data, drive compliance and minimise both cyber and data risk.

Put simply, the paper aims to demonstrate that knowing your business's data needs and compliance obligations enables you to build an information governance framework that can then be run using compatible technology that is adaptive to change.

Introduction

Australian and global corporates have never been under greater scrutiny to act in relation to their use and protection of data, both to maximise opportunities and minimise risk. The spate of major data breaches across Australia has revealed fundamental flaws in current approaches to, and understanding of, information management, and in particular, personal information.

Amendments to the *Privacy Act 1988* (Cth) were expedited following the Optus and Medibank data breaches, increasing penalties to the greater of $50 million, three times the benefit obtained from the breach or 30% of adjusted turnover in the relevant year.

Further privacy changes are firmly on the agenda based on the Privacy Act Review Report, released in 2023. As a result, Corporate Australia's focus on privacy has sharpened dramatically.

Balancing opportunity and risk

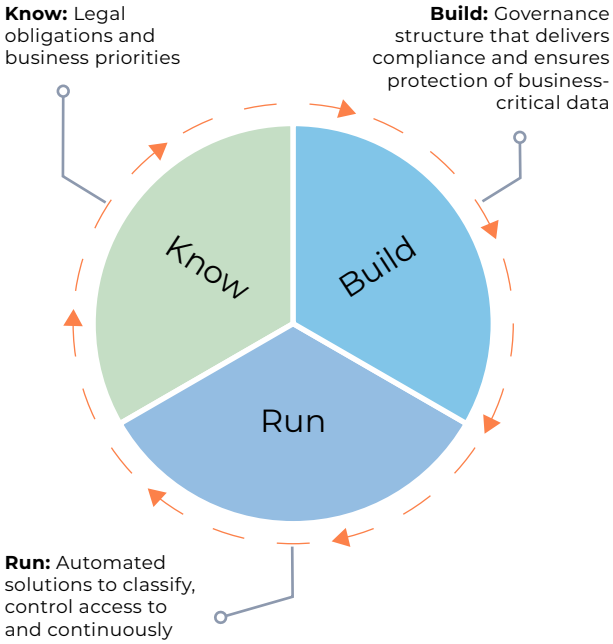
Organisations are increasingly realising that the value of data can be vulnerable to erosion from a cyber attack, turning its potential for profit into customer churn, class actions, regulator intrusion, fines and damage to reputation. There is also an increasing awareness of the relationship between data risk and directors' duties. Each of these factors have seen data and cyber now forming a central pillar of corporate governance and an essential role in corporate strategy.

In today's world, the need to use data is enterprise-wide, yet the responsibility for it has often fallen to the chief technology officer (CTO) or risk and compliance functions. This assignment of responsibility is proving to be increasingly outmoded in a rapidly changing threat and duties landscape.

Know, Build, Run

In this white paper, leading experts from legal advisory, cyber and data security consultancy and artificial intelligence technology disciplines propose effective and reliable approaches to data management to better navigate the reality of enterprise-wide needs for data and the associated enterprise-wide risks that arise.

Diagram 1: this tripartite solution is best represented as a circle of action that enables organisations to know, build and run effective and cost-efficient data governance.



Specifically, this approach enables organisations to:

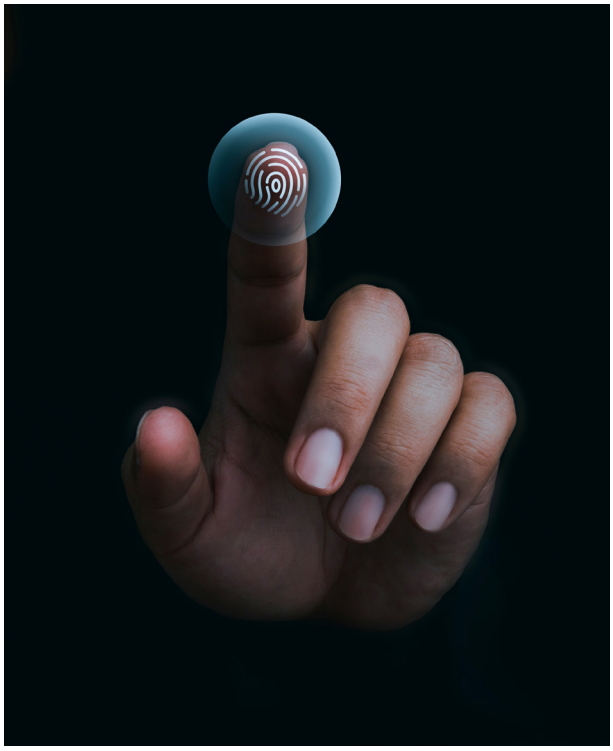
- **Know** your legal compliance obligations including updates and changes;
- **Build** a governance framework that is legally compliant and prioritises data required to do business; and
- **Run** automated data classification, manage access control and continuous data monitoring.

Navigating the paper

This white paper is divided into three sections :

- **Section one** is about ***knowing*** the duties landscape and the legal developments in Australian privacy law.
- **Section two** focuses on ***building*** a governance framework that is informed by applicable legal obligations and is responsive to evolving information security threats. Specifically, it provides an outline of an information governance framework that organisations can adopt to manage data in a structured manner, and provides operational guidance on supporting compliance.
- **Section three** focuses on ***running*** or operationalising an information governance framework using the benefits of modern technology to automatically classify data, implement controls and ensure continuous monitoring of all data assets.

You are invited to explore these themes in detail throughout the document and reach out to the authors should you have questions.



Authors

Lisa Fitzgerald
Partner, Digital Economy - Corporate
Lander & Rogers

T +61 3 9269 9103
E lfitzgerald@landers.com.au

Broderick Smith
Senior Data Governance Advisor
Intalock

T 1800 996 613
E broderick.smith@intalock.com.au

Peggy Tsai
Chief Data Officer
BigID

E peggyt@bigid.com

Contact
Tim Roughton
ANZ Sales Manager, BigID
T +61 452 235 501
E troughton@bigid.com

Section one: Know

Legal developments in data regulation

Before building an information governance framework that can support corporate strategy, reduce risk and achieve compliance, it is essential to identify and develop a knowledge of applicable data laws. This section summarises the data regulatory landscape in Australia, the tempo of recent and anticipated changes and the activity and appetite of our regulators. The increased pace of data regulation also means that any governance model must be adaptive to change.

Part A: The legal landscape

The legal landscape governing data is vast and evolving in Australia. With most businesses using technology as their modus operandi, data generation and usage is inevitable and increasing. As a corollary, with human beings interacting with technology, information gathering is also inevitable and increasing.

It is important to recognise that data is not a one-dimensional legal consideration. While privacy under the federal *Privacy Act 1988* (Cth) (Privacy Act) is a key risk and personal information is like a moth to the cybercrime flame, data regulation is a hybrid landscape with overlapping regulatory scope and reporting obligations. Accordingly, being advised of the applicable data regulations relevant to your business and sector is indispensable to good corporate governance and plays an increasingly important role in the design and implementation of a data management and optimisation strategy.

Below is a summary of the various laws and regulations applicable to data and information when conducting business in Australia. However, this is by no means an exhaustive list.

Area of law	Legislation
Corporations law	• *Corporations Act 2001* (Cth) • ASX Listing Rules • Directors Duties
Privacy law	• *Privacy Act 1988* (Cth) • Australian Privacy Principles (Schedule 1 to the Privacy Act) Notifiable Data Breaches Scheme (Part IIIC of the Privacy Act)
Consumer law	• *Competition and Consumer Act 2010* (Cth) – Australian Consumer Law – Consumer Data Right • Competition and Consumer (Consumer Data Right) Rules 2020 (Cth)
Financial Services	• *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) • APRA Prudential Standards: Prudential Standard CPS 234 Information Security
Health	• *Health Records and Information Privacy Act 2002* (NSW) • *Health Records Act 2001* (Vic) • *Health Records (Privacy and Access) Act 1997* (ACT)

Area of law	Legislation
Telecommunications	• *Telecommunications Act 1997* (Cth) • *Telecommunications (Interception and Access) Act 1979* (Cth)
Critical infrastructure	• *Security of Critical Infrastructure Act 2018* (Cth)
Government	• *Data Availability and Transparency Act 2022* (Cth)
Contractual	• Data protection and security breach provisions
Confidential	• Common law • Confidentiality requirements under non-disclosure agreements

A focus on privacy law

The processing of personal information is common to all businesses, regardless of sector.

Understanding privacy law is fundamental to ensuring personal information is properly collected and handled in a legally compliant manner. The recent increases to the civil penalty provisions of the Privacy Act, and touted criminal offences for malicious re-identification of de-identified personal information, highlights a shift in the Australian Government's stance on the importance of privacy and its preparedness to act swiftly in the wake of serious privacy breaches.

With significant privacy reforms signalled by the Attorney-General in 2023, below is a summary of the current privacy landscape and where privacy law is heading in Australia.

Current privacy law landscape

Overview: Federal, state and territory dimensions

Federal

The Privacy Act is the primary legislation regulating personal information collected and handled by Commonwealth government agencies and companies with an annual turnover of more than AUD$3 million.

The Privacy Act and its 13 Australian Privacy Principles (APP) regulate how an individual's personal information must be collected and handled by Australian Privacy Principles entities (APP entities).

The APPs are principles-based law that governs the rights, standards and obligations concerning personal information, and the governance and accountability of APP entities that collect and handle personal information.

The Privacy Act also includes some exemptions that relieve compliance with the Privacy Act in certain circumstances. The main exemption is the employee records exemption, which exempts organisations from compliance in respect of personal information directly related to a current or former employee and held in an employee record (section 7B(3)). This may include information relating to an employee's banking and superannuation details, training, membership of professional associations, tax, and personal and emergency contact details.

The personal information of deceased individuals is also exempt under the Privacy Act.

States and territories

Australian local, state and territory government bodies are not covered by the Privacy Act (unless by exception). Most Australian states and territories (excluding Western Australia and South Australia) have equivalent privacy legislation to regulate the state- or territory-based public sector agencies' collection and handling of personal information. In addition, specific state and territory health records legislation regulates the collection and handling of health information of health service providers and organisations.

Scope: what is personal information?

The Privacy Act regulates "personal information", which is defined as:

> *information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not and whether the information or opinion is recorded in a material form or not.*

For example, personal information may be a person's name or address, and can include bank account information, credit history or photos.

"Sensitive information" is a subset of personal information. The Act defines sensitive information as including information or an opinion about an individual's:

- racial or ethnic origin,
- political opinions,
- religious beliefs or affiliations,
- sexual orientation or practices, or
- criminal record
- health or genetic information
- biometric information
- biometric template.

The definition of personal information in Australia is broad in scope. Care must be taken to ensure information is properly classified when assessing whether information is or is not personal information.


1010101010
digital transformation 0;
1010101010101010

Guardrails: the 13 Australian Privacy Principles

There are 13 Australian Privacy Principles that impose a variety of obligations on APP entities in respect of the management, collection, use, disclosure, storage, access and correction of personal information.

The Office of the Australian Information Commissioner (OAIC) has a set of guidelines that outline the APPs and key concepts in detail. The guidelines also outline how the OAIC interprets the APPs, including what the OAIC may consider when exercising its power to conduct privacy assessments of APP entities.

Key princples: APPs 8 & 11

Australian Privacy Principles 8 and 11 are of fundamental relevance to most businesses today.

APP 8: Cross-border disclosure of personal information

Australian Privacy Principle 8 (APP 8) provides a framework for the cross-border disclosure of personal information from Australia to an overseas recipient. Most businesses using cloud services may involve a transfer of data to servers located overseas and many operators of such servers will have access to, or the ability to exercise some form of control over, personal information, if only in the context of responding to a local law enforcement request.

APP 8 sets out the steps an APP entity must undertake before disclosing personal information to an overseas recipient. Generally, an entity must take reasonable steps to ensure the overseas recipient of personal information does not breach the APPs in relation to the information.

APP 8 applies to the "disclosure" of personal information, as opposed to transfer. However, the distinction is far from clear in the context of overseas operators and their duties to comply with their local laws that may be in contradiction to Australian laws.

Unlike other privacy laws, such as the General Data Protection Regulation (GDPR), the Privacy Act does not set out a prescriptive method or minimum contractual terms for disclosing personal information overseas, nor expressly recognise foreign laws as imposing adequate protections equivalent to the Privacy Act.

APP 11: Reasonable steps and data retention

APP 11 is an elemental obligation for APP entities and an important area of focus for compliance efforts.

A spate of data breaches across corporate Australia in 2022 points to the need for a more detailed understanding of 'taking reasonable steps' in respect of the security of personal information, data retention and obligations under APP 11.

Understanding APP 11

APP 11 requires APP entities to take an active approach to data security, retention and destruction. Under the principle, an APP entity that holds personal information must take reasonable steps with respect to the circumstances to protect the information from misuse, interference, loss and from unauthorised access, modification, or disclosure.

It requires an APP entity to take reasonable steps to destroy or de-identify the personal information it holds once the personal information is no longer needed for any purpose for which it may be used or disclosed under the APPs or under an Australian law.

There is no specific data retention period established under the Privacy Act. However, APP entities must comply with APP 11 in relation to destroying or de-identifying personal information that is no longer required by the APP entity or is permitted to be retained under an Australian law.

Following the Optus data breach in September 2022 and the Medibank data breach in October 2022, the OAIC initiated investigations into the personal information handling practices of both companies. In both investigations, there is a focus on whether reasonable steps were taken to protect personal information and whether the Australian Privacy Principles were adequately complied with by Optus and Medibank.

Australian privacy regulators

The Office of the Australian Information Commissioner (OAIC) is Australia's privacy regulator and oversees the functions of the Privacy Act. Australian states and territories also have their own privacy regulators.

Data breach notification

Under the Privacy Act, serious data breaches that satisfy certain conditions, must be notified to the OAIC and affected individuals.

Australia's Notifiable Data Breaches (NDB) scheme applies to an eligible data breach, which occurs where:

- an organisation or agency holds personal information (s 26WE(1));
- there is unauthorised access to or unauthorised disclosure of the information (s 26WE(2)(a)(i));
- it is likely to result in serious harm to one or more individuals (s 26WE(2)(a)(ii)); and
- remedial action has not been able to prevent the likely risk of serious harm (s 26WF).

The Notifiable Data Breaches scheme applies to breaches that occurred after 22 February 2018, or where data may have been accessed after that date.

As soon as an APP entity is aware that there are reasonable grounds to believe that it has suffered an eligible data breach, affected individuals and the OAIC must be notified of the breach.

There are also a variety of additional notification obligations for certain organisations under other pieces of legislation.

For example:

- The *Security of Critical Infrastructure Act 2018* (Cth) requires responsible entities of critical infrastructure assets to report cyber security incidents to the Australian Cyber Security Centre;
- The Australian Prudential Regulation Authority's (APRA) *Prudential Standard CPS 234* requires APRA-regulated entities to notify APRA when material information security incidents occur; and
- The ASX listing rules require listed entities that experience data breaches to disclose the breach to the ASX if the breach is reasonably expected to have a material effect on the price of the company's securities.

Recent changes to the Privacy Laws

In response to the Optus and Medibank breaches in Australia, *the Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022* (Amending Act) was fast-tracked and received royal assent on 12 December 2022. The Amending Act implements the most significant reforms to Australia's privacy laws since the commencement of the Notifiable Data Breaches (NDB) scheme in 2018.

The Amending Act amends the Privacy Act by:

- expanding the extraterritorial reach of the Privacy Act. Foreign organisations no longer need to collect or hold personal information in Australia or an external territory to be bound by the Act. Overseas businesses that carry on business in Australia, or an external territory, are bound to comply with the Privacy Act.
- significantly increasing penalties for serious or repeated interferences with privacy, to the greater of:
  - $50 million;
  - three times the value of the benefit obtained from the conduct constituting the serious or repeated interference with privacy, if the court can determine this value; or
  - 30% of the body corporate's adjusted turnover in the relevant period, if the court cannot determine the value of the benefit.
- strengthening the NDB scheme. The OAIC is now able to:
  - request information and documents from an APP entity about actual or suspected eligible data breaches; and
  - conduct assessments of an entity's compliance with the NDB scheme.
- enhancing the powers of the OAIC to investigate and resolve privacy breaches, particularly in relation to making determinations following an investigation of a complaint. The Commissioner is now able to:
  - require a person or entity to engage an independent adviser following the investigation of a complaint;
  - require a person or entity to publish a statement with details of conduct and steps taken to remediate an interference with privacy;
  - issue infringement notices where an entity fails to provide information without a reasonable excuse; and
  - issue penalties for systematic failures to provide information.

Attorney-General's Department review of the Privacy Act

What is on the horizon?

On 12 December 2019, the Attorney-General announced a general, wide-ranging review of the Privacy Act. The review examined the scope and enforcement mechanisms in the Act to ensure that consumers are empowered, and their data protected, by the current privacy settings. It also examined whether the current settings are what is best to serve the Australian economy.

The Privacy Act review was completed in late 2022 and the Attorney-General's Department delivered its final report as part of a consultation report in February 2023.

Among its 116 proposals, the report gives serious consideration to the introduction of a right to be forgotten (erasure), a statutory tort for serious invasions of privacy, technical and organisational measures to achieve baseline security and satisfy reasonable steps under APP 11 and other baseline outcomes following consultation informed by the 2023-30 Australian Cyber Security Strategy (as outlined in the Government's discussion paper at the time of writing).

PART B: CONVERGENCE OF LAWS

Privacy and data protection is multi-dimensional and enlivens a range of legal obligations and considerations. The various laws noted above highlight the complex regulatory framework that applies to data and personal information in Australia. Given this complex regulatory environment, it is unsurprising that various Australian regulators are becoming increasingly more active in the privacy and data regulatory arena.

Businesses are also facing a new frontier in data breach class actions.

Consumer and privacy laws

Privacy and data protection is no longer just a privacy issue, it is also a consumer law issue.

Since the completion of the Australian Competition and Consumer Commission (ACCC) digital platforms inquiry in 2019, the ACCC has been proactive in pursuing companies (in particular digital platforms) engaging in privacy practices that are misleading or deceptive to consumers.

In April 2021, in the case of the *ACCC v Google LLC (No 2)* the Federal Court of Australia found Google misled consumers about the collection of their personal location data through the use of Android mobile devices between January 2017 and December 2018. The Federal Court ordered that Google pay $60 million in penalties for misleading and deceptive conduct in contravention of the Australian Consumer Law (ACL).

This case is significant for several reasons.

1. Firstly, it demonstrates the ACCC's willingness to undertake enforcement action against companies that mislead customers about how their personal data is being collected and used.
2. Secondly, it illustrates how the ACL, with its substantial penalties, may be used as an alternative to privacy law in protecting individuals from improper collection and use of their data.

Regulators are working together and sharing intelligence

The protection of personal information and the regulation of digital platforms is a regulator priority. The ACCC, Australian Communications and Media Authority (ACMA), Office of the Australian Information Commissioner (OAIC) and the Office of the eSafety Commissioner have formed the Digital Platform Regulators Forum. The Forum brings together Australia's regulators to share information and collaborate on the regulation of digital platforms, including in relation to privacy and data issues.

It is evident from recent regulator activity that privacy and data protection is a multi-dimensional issue grabbing the attention of multiple Australian regulators. Consequently, businesses can no longer manage privacy risk in a siloed manner.

Common law, corporations and directors

Directors' duties and their relevance to cyber and data protection

Under the *Corporations Act 2001* (Cth) (Corporations Act), directors are required to exercise their powers and perform their functions:

- in good faith including acting in the best interests of the company;
- with care and diligence; and
- without using their position or information to gain personal advantages (ss 180, 183, 601FD).

These statutory duties derive from long-standing common law fiduciary duties and the essential duty of due care and skill. While "due care and skill" is not defined in the Corporations Act, the expectation on directors to be technology and data literate is increasing alongside the growing dependency upon technology and the data that drives it.

RI Advice decision - corporate Australia on notice to uplift cyber security practices

The Federal Court's decision in *Australian Securities and Investments Commission v RI Advice Group Pty Ltd* [2022] FAC 496 highlights the potential need for financial services and corporate sector businesses to do more to reduce cyber risk and strengthen security posture. This is the first time an Australian Federal Court has ruled on cyber security risk and cyber resilience in connection with Australian Financial Services Licence (AFSL) conditions, with significant implications for corporates, particularly APRA-regulated entities, using technology and handling personal, sensitive, financial and confidential information.

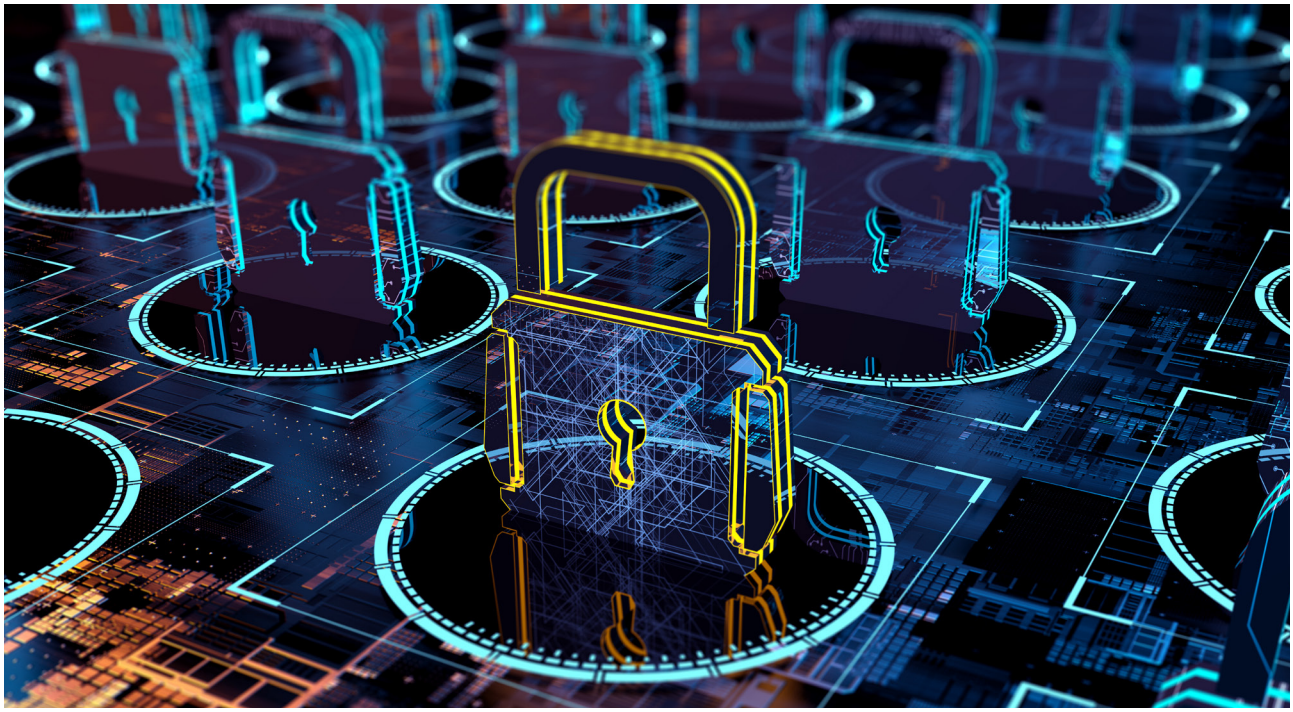
The decision has changed the course of cyber security in the Australian financial services sector and elevated the role of independent cyber security experts. While civil penalties were not issued on this occasion, both ASIC's action and the Federal Court's decision make clear that penalties will almost certainly be invoked in future where circumstances permit.

Rise of class actions

Data breach class actions have historically been difficult to pursue in Australia. It is challenging for claimants to commence and successfully bring court action in respect of a data breach due to the difficulties in identifying a cause of action. Australian law does not recognise a statutory right to privacy or tort of invasion of privacy. As such, other potential causes of action need to be identified, such as breach of contract, breach of confidence and misleading or deceptive conduct.

Only one class action has succeeded in Australia. In *Evans v Health Administration Corporation* [2019] NSWSC 1781 the New South Wales Supreme Court approved a settlement of AUD$275,000 awarded in the claimant's favour.

Recent major Australia data breaches have resulted in law firm investigations into potential class action claims, serving as a reminder that companies that suffer large scale data breaches are at risk of class action claims.



Summary of Australian privacy law

Australia's privacy laws may soon resemble, and in some cases surpass, the onerous obligations set by the General Data Protection Regulation (GDPR) in Europe.

While increased regulatory fines alone may not force a change in data governance practices, there are several considerations that are likely to move the dial including:

- the reputational damage that immature data governance and security posture can bring following a cyber attack;
- the potential introduction of a personal right of action and the rise of the class action;
- the potential obligation to identify and destroy personal information on request and reconcile this against data retention obligations and other legal considerations;
- the increased risk of regulator intervention to audit and prescribe remediation programs; and
- the weight of customer expectation and consumer confidence for the compliant and ethical use of personal information.

These considerations are important for those empowered to make decisions about corporate governance and how to appropriately discharge directors' duties.

More than ever before, now is the time for organisations Australia-wide to:

- review applicable data-related regulations; and
- make informed decisions about compliance, data retention, deletion capabilities, identification of data essential to business operations, corporate strategy and corporate governance.

Understanding the wide-ranging threats that may impede compliance and responsiveness is an inevitable part of that review and will lead to a governance framework that works to support business growth, minimise risk and drive compliance.

Section two: Build

Compliance and responsiveness in an evolving threat landscape

Criminals now work at machine speed

Traditionally, cyber attacks are calculated: cyber criminals often spend significant time researching and gathering information about their targets before launching an attack. This reconnaissance can take days, weeks or even months before launching the attack or gaining entry to an organisation's system.

More contemporary techniques are increasingly employed by cyber criminals including automated processes and machine-speed operations, which use bots or other pre-programmed software to scan networks for vulnerabilities, launch phishing attacks, or carry out distributed denial of service (DDoS) attacks.

All of these methods use banks of server and computing power to automate the discovery and interrogation of thousands of organisations' systems per second - all pre-programmed and fully automated. Once inside an organisation, threats actors are able to automatically execute a new set of programs to further investigate vulnerabilities.

One of the most common machine-speed attacks is ransomware, which uses encryption algorithms that execute at machine-speed to encrypt the victim's files.

The rise of information security

Information security and cyber security are related fields, and historically the terms are often used interchangeably. However, information security is a broader concept that encompasses all aspects of protecting information including legal compliance and digital assets.

Cyber security specifically focuses on protecting digital systems and networks from cyber threats. The concept of information security encompasses not only protecting digital systems and networks, but also physical security measures, access control, data governance, risk management, and other related areas. It is therefore a broader and more holistic approach to protecting information that considers a wide range of factors, rather than just focusing on cyber security measures.

In recent years, there has been a growing emphasis on information security and the need to protect sensitive data and information from unauthorised access, theft, and other threats. This is due to various factors, including the increasing amount of sensitive information being stored and processed electronically, the growing number of cyber attacks and data breaches, and the increasing regulatory requirements and compliance obligations related to data protection.

Corporate governance

Boards are under increasing pressure to better manage data risk and drive data value.

In those data-mature organisations, information governance frameworks or strategies are being developed to support this process. Still, there are some important questions to determine from the outset: 'who' within an organisation is best placed to own strategy development and delivery, 'how' is a fit-for-purpose data framework designed and 'what' data should be classified and fall within the scope of the framework.

Data, information, information management and governance

Data can be simply defined as ones and zeros – a value in a database field, a word in a document, whereas **information** can be defined as data with purpose – the combination of data elements that has value and that the business can utilise.

Data should be properly classified and managed to extract the maximum business value for the customers and stakeholders.

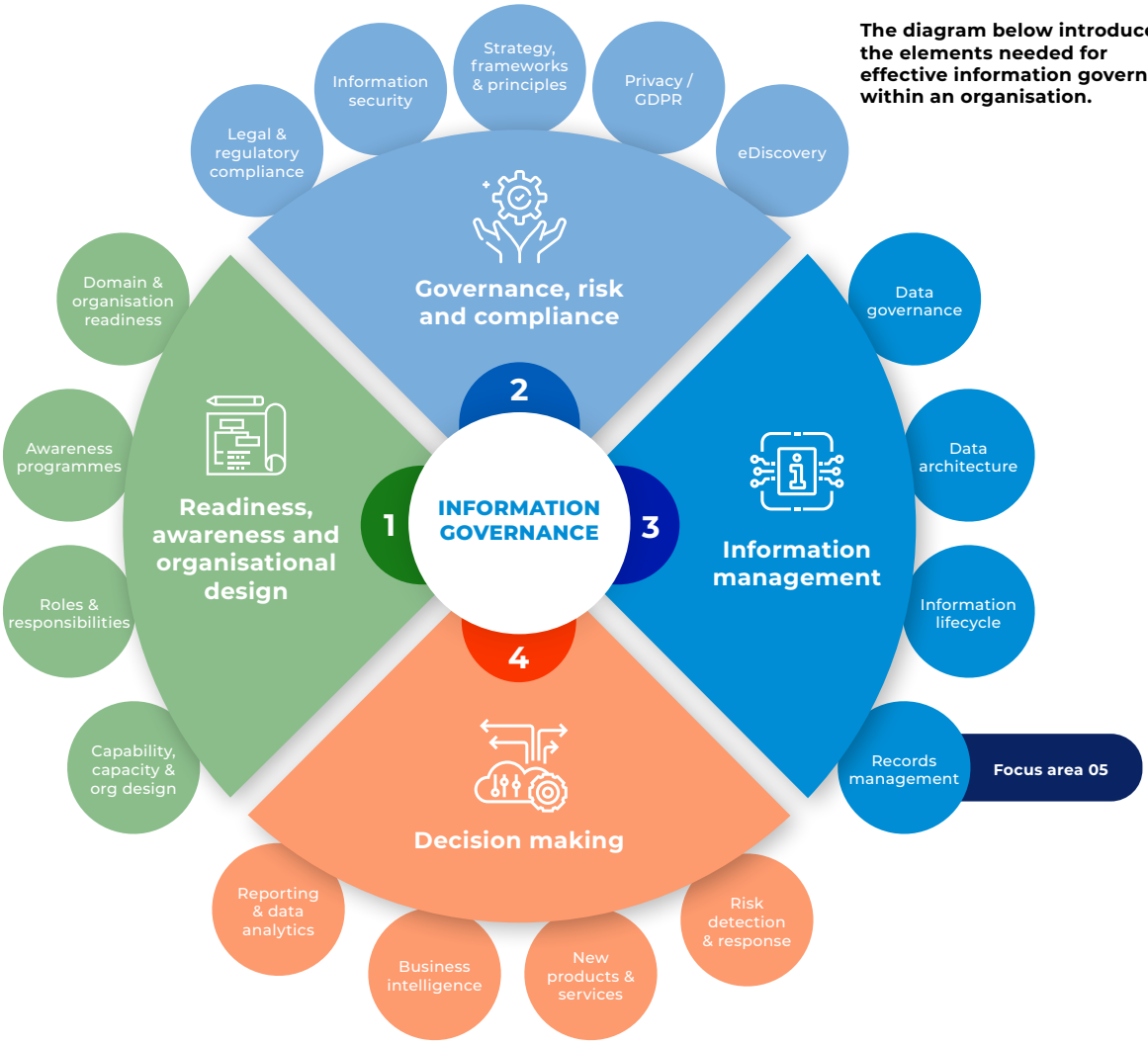
Information management is the process of collecting, storing, using and disposing of data in a way that is both efficient and effective.

It is a critical function for businesses of all sizes and industries. Data is a valuable asset that can be used to make informed decisions, improve internal business operations, and drive growth.

Information governance describes how information is to be governed as an asset of the organisation., The business' operating environment (social, technological, political, regulatory and economic factors) informs the requirements of the business' strategic, tactical and operational instruments including policies and standards.

Information governance framework

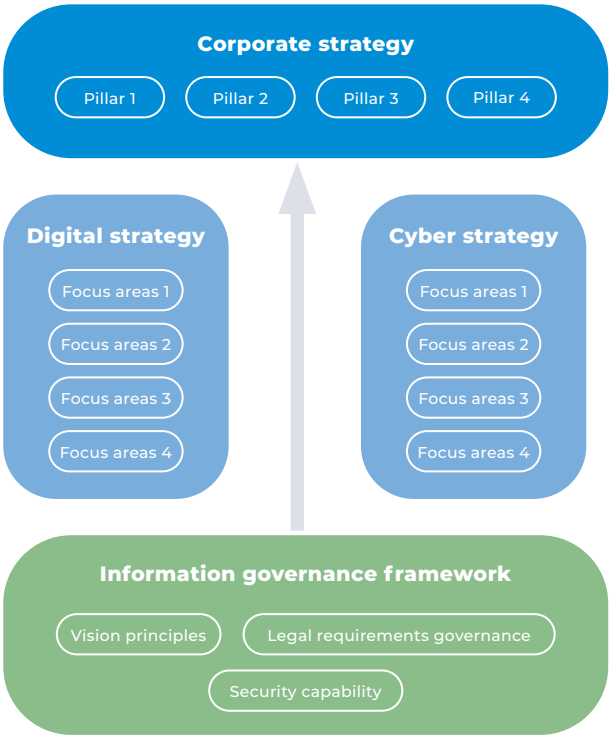
The diagram below introduces the elements needed for effective information governance within an organisation.



Implementing all of the elements of an information governance framework can be complex and time-consuming, especially as the organisation grows and the volume of data increases at an unprecedented rate. In addition, new data types and sources, especially in unstructured formats, can represent potential personal and sensitive data risks.

Before considering future information management programs, organisations should set and clearly understand two important components:

1. the organisation's awareness of information governance and readiness to tackle such a program; and
2. the organisation's strategic objectives. Any information governance and management initiatives must complement and operate in alignment with the organisation's strategic vision and future digital strategy. Strategy drives the initiatives and initiatives drive the projects required to deliver the strategic objectives. Ideally, the strategy related to information and governance mechanisms must be clear and complete before commencing any project.



An information governance framework

An information governance framework is the business operating, legal, and regulatory context within which information assets are created, used and managed. Generally, a business has several drivers that dictate the requirements for a framework including:

- understanding regulatory obligations and associated legal risk.
- understanding the business context of information assets.
- communicating clear guiding principles that reflect an approach and commitment to creating, managing, using, securing and disposing of information.
- aligning information strategies to a newly established policy set to build the organisation's operating objectives.
- outlining the roles and responsibilities for information management within the organisation.
- assessing business system functionality against standards to consider business information system needs, risks, opportunities and ultimately control enhancement, to improve information security, and
- identifying resource requirements for information governance planning and management.

An information governance framework should outline the following key elements:

1. Overview;
   a. Purpose,
   b. Scope,
   c. Objectives.
2. Organisational information principles;
3. Governance framework (environmental commentary);
   a. Broader organisational and operational environment,
   b. Legislation, standards and policies,
4. Information management policy;
5. Information management strategies;
6. Business' information systems;
7. Roles and responsibilities;
8. Review;
9. Authorisation.

An information governance framework has many benefits including:

- the establishment of goalposts to guide and facilitate compliance controls and ensure compliance obligations are met (such as adherence to the Privacy Act);
- the protection of organisational proprietary information;
- limiting the accidental creation of organisational knowledge;
- increasing speed and efficiency in the effort required to locate and access relevant, complete information, and share it across the organisation (including e-discovery requirements);
- mitigation of risks that arise from poor information governance practices or non-compliance with legislative and regulatory obligations. For example, reducing risk of a data breach and subsequent reputational risk or financial penalties;
- improved service delivery; and
- a solid foundation for future digital strategy and support for the corporate strategic vision.

Roles and responsibilities

Roles and responsibilities are a fundamental component of an organisation's information governance framework. They define each party's obligations in the management and use of information for business-as-usual (BAU) purposes.

Common information management roles are as follows:

- **Information owner** - Information owners have enterprise-level authority and accountability for collecting and managing an organisation's information.
- **Information leader** - Information leaders provide strategic guidance regarding information requirements within one or more information domains.
- **Information custodian** - Information custodians define and implement safeguards to ensure the protection of information within their information domain. This must be performed following the policies, procedures and rules approved by the information owner or information leaders.
- **Information steward** - Information stewards are responsible for the quality, integrity and use of the information assets within their information sub-domain daily. An information steward may manage multiple information assets.
- **Information creator** - Information creators capture or create the information as defined by the information domain custodian.
- **Information consumer** - Information consumers select the best source of information to meet their requirements for use.

At the board level, directors oversee an organisation's information governance framework.

In addition to informing the strategic direction of an information governance framework, directors must observe their directors' duties. These duties are not static and evolve in accordance with changes in the risk landscape, technological advances, and shareholder expectations. While requirements for a director's digital literacy may not extend to mastering what many would compare to a foreign language (in the form of artificial intelligence; algorithms; data sets, hygiene and transfer; biometrics; behavioural data; the latest ransomware or dark web activities), being properly advised of data management and risk is a key requirement for directors.

It stands to reason that a board or equivalent structure should oversee an organisation's information governance framework development, and be aware of the associated benefits and risks, including legal risk. The ongoing management of the information governance framework should sit with a specialised committee of key organisational stakeholders. While this does not transfer a director's liability, nor can a director rely absolutely on the advice of employees, advisors or a committee, being properly advised on data risk in a technological environment is important to dispensing directors' duties.

Aligning an information governance framework to legal obligations

As outlined in the previous section, an information governance framework must be informed by relevant laws discovered in the 'know' stage.

The information governance framework must be aligned to and outline all relevant legislation and regulation - such as privacy laws, sector specific regulations, cyber security laws and contractual obligations.

Assessing and understanding the legal risks or liabilities of a data strategy is a key component to the success of a strategy. Unfortunately, information governance frameworks are often established without full regard or appreciation of the full spectrum of legal issues or risks that may impact on successful operation of the framework. That is why it is important to properly identify and classify data and map it to sources and to relevant laws.

Managing risk

An information governance framework incorporates risk management tools or assessments to assist organisations with regulatory compliance, particularly privacy compliance.

Privacy impact assessments or PIAs provide a systematic framework to identify and assess the privacy impacts a particular project may have on individuals. PIAs are an important tool that can be used to identify and mitigate privacy risks.

The development and adoption of privacy technology is on the rise. New solutions enter the market each year to assist organisation with privacy compliance within an organisation.

Automation compliance tools, such as Lander & Rogers PrivacyComply, enable organisations to manage privacy risk and compliance more efficiently by moving away from paper-based systems to cloud solutions.

The importance of understanding data holdings

Organisations generally have a vast number of disparate systems that store data and information. Organisations rarely know the quantity of information assets contained within these disparate systems and in many cases have no confidence over the number of disparate systems within their environments. A system register and an information asset register are two necessary artefacts that assist organisations to understand different platforms and datastores used within the business, and the types of information that exists within these data stores.

An information asset register (IAR) is a structured inventory of all the important information assets owned and managed by an organisation. It is essentially a document that contains a list of all the information assets, such as data, documents, software, and hardware, that an organisation uses to achieve its business objectives.

An IAR provides an understanding of where information resides, where it has originated, its confidentiality, integrity and availability needs, importance to the business, and data ownership and custodianship, and ultimately allows the organisation to build controls around its data. The IAR is an important component of information governance and information security management. It is used to gain visibility and fully understand the lifecycle of an information asset from creation to destruction.

The information recorded in an IAR can support a range of activities, such as:

- duplication
- accessibility and usage,
- risk management
- compliance,
- audit, and
- incident management.

It can also help organisations make informed decisions about information management and improve information security.

Building an IAR via manual methods can take months as it involves working with every business unit within the organisation to workshop and build a library of information on critical assets. Automation is critical to maintain the freshness of the assets as well as help provide controls around security and privacy compliance.

Gaining visibility of corporate data

Content and context

Even if an organisation understands its different systems and data sources, there are numerous questions about data that organisations must be aware of.

For example, are certain data types stored improperly including the housing of account credentials in spreadsheets, sensitive configuration files in unrestricted locations, or certificates stored on network drives?

It is this type of data that should be monitored, and RFDS alerted to if it exists now or is inadvertently newly created and stored in the future.

The key objectives of data discovery include:

1. **identifying all sources of data:** One of the primary objectives of data discovery is to identify all the sources of data within an organisation. This includes structured and unstructured data, such as databases, spreadsheets, email, and social media.
2. **Understanding data lineage:** Another key objective of data discovery is to understand the lineage of data, i.e., how data is created, stored, used, and disposed of. This helps organisations ensure data quality and compliance with regulations.
3. **Assessing data quality:** Data discovery also helps organisations assess the quality of their data. By understanding the sources of data and its lineage, organisations can identify any data quality issues and take steps to improve data quality.
4. **Managing data security risks:** Data discovery can help organisations identify data security risks, such as unauthorised access or data breaches. This allows organisations to take appropriate measures to mitigate these risks and protect sensitive data.
5. **Supporting regulatory compliance:** Data discovery is crucial for organisations to comply with various regulations, such as GDPR, HIPAA, and CCPA. By identifying all sources of data and understanding data lineage, organisations can ensure compliance with these regulations.
6. **Enabling better decision-making:** By discovering and analysing data, organisations can gain insights that enable better decision-making. This can help organisations improve operations, increase revenue, and reduce costs.

Gaining visibility of data assets is a critical initial activity towards good data security and privacy compliance. And must be undertaken before embarking on information security initiatives such as classification.

Data classification

Information must be classified to protect the data discovered within the corporate environment.

Different data types have different sensitivity levels which dictate different levels of protection. Appropriate security controls can be implemented based on the sensitivity of the specific data. For example, highly sensitive data may require encryption or limited access controls to ensure that it is only accessible to authorised personnel, whereas less sensitive data that is already in the public domain may not require such stringent security measures.

Control mechanisms such as data loss will use information classification to control data access, usage and transport in and outside the business. Data loss prevention (DLP) can prevent sensitive information from being accessed by people who are not the intended audience within and even outside of the business.

Protecting Information at rest and information in motion

Protecting information at rest and protecting information in motion are two different concepts of information security. Threats to privacy and information don't only originate from outside the organisation – malicious or purposeful attempts to access restricted data can be from legitimate employees of the business. In addition, external cyber criminals often use the credentials of employees to access data once inside the organisation's systems.

Information at rest refers to data that is stored or archived on devices such as hard drives, USB drives, servers, or cloud storage. Protecting information at rest involves measures such as encryption, access controls, authentication, and backups as detailed below.

Protecting information at rest ensures only authorised uses can access specific types of information.

Information in motion, on the other hand, refers to data that is being transmitted or communicated between devices or networks. Protecting information in motion involves measures such as encryption, firewalls, intrusion detection and prevention systems, and secure protocols.

Encryption ensures that the data is secured during transmission and cannot be intercepted by unauthorised parties. Firewalls and intrusion detection and prevention systems are used to protect against unauthorised access to the network or data during transmission. Secure protocols such as SSL/TLS ensure that data is transmitted securely over the internet.

In summary, protecting information at rest and protecting information in motion serve different purposes but are both important to ensuring the confidentiality, integrity, and availability of data.

Steps to protect information at rest.

- Encryption ensures that data is secured through encryption algorithms, making it unreadable to unauthorised users.
- Identify-and-access management ensures users trying to access data have been fully identified against known parameters. It also validates the machine they are using and other aspects like geo-location to verify via a risk assessment that it is actually the user they claim to be.
- Access controls mechanisms are used to limit access to the system, folder or data to authorised users only.
- Classification of data ensures that certain users can access only certain types of data – for example if using business classification, a HR officer cannot access finance data, no matter where it is stored. If using security classification, a standard user cannot access data labelled as protected.
- Backups are used to ensure that data can be restored in case of data loss or corruption.

Operationalising

Ultimately, the information governance framework will be delivered through organisational policy. Policy statements will include aspects detailed above in order to discover, classify and protect information at rest and in motion.

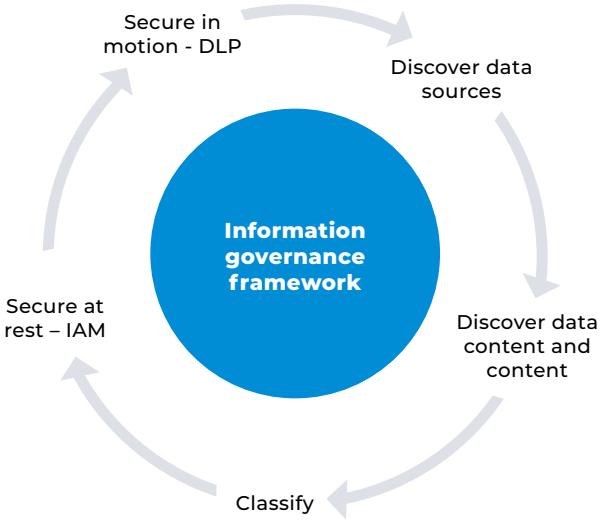
Discovery and classification activities can be performed manually or through pattern matching queries. These traditional methods are time-consuming to create and to monitor. For example, it may take several months to document the rules and implement into various production phases, ranging from workshopping to coding.

Modern tooling leveraging machine learning and artificial intelligence such as BigID's data discovery platform, can streamline the manual discovery process and make discovery a simpler process across multiple structured data sources, whether on-premise or in cloud-based software-as-a-service (SaaS) applications.

This is far superior to traditional methods of manual and pattern matching processes that fail to provide control and audit trails over discovering unstructured data sources, which is a growing source of risk in all organisations.

If discovery is managed correctly at the onset of any data management or governance framework, data classification can be easily applied to enforce a policy and control-set perspective in many business applications such as Microsoft 365.

Advancements in modern technology have made data discovery and classification efficient in supporting information data stewards and more consistent in applying consistent policies and controls compared to traditional manual methods.




[B1]
[B2]
Personal Data User 0001
Personal Data User 0002
Personal Data User 0003
Personal Data User 0004
[B3]
Personal Data User 0005
User Admin 0002
IOT

Section 3: Run

Automated discovery, classification, controls and monitoring

Working at the same speed as criminals

Cyber criminal tactics continuously evolve, becoming increasingly more sophisticated by utilising the latest technology. From developments in hardware to advancements in software like artificial intelligence, the constant state of change makes it challenging for organisations to stay ahead of the game in guarding against cyber threats.

While technology can pose a threat, it also represents one of the best defences for organisations in response to cyber threats. While no panacea, technology like machine-speed tools can help automatically detect and respond to threats, providing organisations with the necessary tools to proactively manage cyber risk and protect data.

Software

Automated threat-detection systems and artificial intelligence are increasingly being used to detect and respond to attacks in real-time. Therefore, the speed of the attack is not the only factor that determines whether a cyber criminal is successful.

The sophistication of attacker techniques, their ability to bypass security measures, and the effectiveness of the security controls in place are all important factors that can impact the outcome of a cyber attack.

Software can assist in automating the discovery of all information assets within an organisation, and are specifically helpful in detecting sensitive personally identifiable information (PII) across the realm of information stores within a business, whether on-premise, in the cloud or in third-party databases.

Discovery software uses various techniques to identify specific information assets. These techniques include:

- **Business glossary:** this is the simple function of documenting and establishing consistency of definitions pertaining to the type and use of data. It refers to predefined lists of sensitive information types and terms, such as names of individuals, organisations, and addresses.
- **Keyword and pattern matching:** the software searches for predefined keywords and patterns within data, such as social security numbers, credit card numbers, or dates of birth, to identify sensitive information. This can result in false positives if strings of numbers can be confused for account numbers or product license codes.
- **Machine learning algorithms:** the software uses advanced algorithms, such as natural language processing (NLP) and machine learning, to analyse and categorise data based on its context, content, and structure. This can lead to a higher confidence score for accuracy if the algorithm can learn from the original data and if the end-user can provide feedback to teach the algorithm.
- **Context analysis:** the software considers the context in which data is used to determine if it is sensitive in nature. For example, an employee's salary information may be sensitive within the context of a company's HR records, but not within their own personal financial records.

Software and smart tooling can assist organisations to obtain a clear picture of all data sources in use. In many cases, organisations know of their own internal or sanctioned cloud storage systems. However, 'shadow IT' data sources may be in use beyond the IT or security team's knowledge, and therefore classification and DLP techniques will not have been applied.

Shadow IT often arises because employees are looking for new, innovative and efficient ways to work, and are using technologies that they believe will help them be more

productive. However, this can create security and compliance risks for the organisation, since these technologies may not have been vetted for security or compliance in accordance organisational policies.

Software can assist in detecting shadow IT and other data sources using the following techniques:

- **Network traffic analysis:** This technique involves monitoring network traffic to identify data sources and patterns of data transfer. This can be used to identify suspicious activity, such as the transfer of data to an unauthorised location or identifying quantity of data larger than the user's normal daily average, which may indicate something suspicious.
- **Endpoint monitoring:** This involves monitoring activity on individual devices, such as laptops or mobile phones, to identify data sources and patterns of data use. This can be particularly useful for detecting insider threats or other malicious activity.
- **Cloud access security brokers (CASB):** CASBs can provide visibility into an organisation's cloud services and applications, and can help identify sensitive data stored within those services. CASBs can also provide controls to prevent unauthorised access to cloud data.
- **Data mapping and flow analysis:** This technique involves mapping the flow of data through an organisation's network, including the sources and destinations of the data. This can help identify areas of the network that are particularly vulnerable to data loss, and can inform the development of DLP policies and controls.

Once data sources are discovered, software can also then assist in automatically classifying sensitive information according to the organisation's business classification schema or information security classification framework. The software can automatically apply labels, metadata, or encryption to the identified sensitive information to secure and manage it appropriately in alignment with an organisation's data loss prevention policy.

Software can then control the usage and transport of data, via data loss prevention techniques (DLP), both within the four walls of the organisation and also outside the four walls of the organisation, ensuring PII or corporate sensitive data can be restricted to certain organisations, people or even down to the ability for someone to print or forward the email outside of the organisation.

Software can assist in DLP automation by managing and monitoring data loss in many ways, including but not limited to:

- **Monitoring network traffic:** DLP tools can monitor network traffic to identify and analyse data in motion. This can help identify sensitive data that is being transmitted, and can alert security teams if any suspicious or unauthorised activity is detected.
- **Enforcing access controls:** DLP tools can enforce access controls to limit who can access and transmit sensitive data. For example, DLP tools can prevent users from sending emails or files to unauthorised recipients, or can require multi-factor authentication to access sensitive data (internally and/or externally).
- **Applying encryption:** DLP tools can apply encryption to data at rest and in motion to protect it from interception or access once outside the four walls of the organisation;
- **Blocking unauthorised data transfers:** DLP tools can identify and block unauthorised data transfers, such as attempts to send sensitive data to external email addresses or cloud storage services. This can help prevent data breaches and intellectual property theft.
- **Analysing content of data in motion:** DLP tools can analyse the content of data in motion to identify sensitive information if the file has not yet been classified, such as credit card numbers or personally identifiable information (PII).

By combining these automated techniques, software can provide a comprehensive and automated solution for detecting sensitive information and ensuring its protection.

Artificial intelligence as an assistive technology

Artificial intelligence (AI) has been rapidly advancing in recent years and is becoming an increasingly important tool for businesses in all industries. One area where AI has the potential to make a significant impact is in data lifecycle management from discovery and governance through to remediation and deletion of data. If implemented correctly in the business, AI data management has potential benefits in relation to data protection, risk management, compliance reporting, data monetisation and more.

Automated data discovery to increase data governance scope coverage

One of the ways in which AI data management can assist with privacy compliance is through the use of automated data discovery and classification tools. These tools can be used to identify and classify personal information within an organisation's data, and can be configured to automatically detect and flag data that is not compliant with the policies. Therefore, regardless of changing privacy compliance and cyber security threats, automation discovery tools such as BigID, can actively monitor for these changes.

The accuracy of AI has improved significantly in the past few years to correctly utilise context to differentiate between names and cities as an example. Rudimentary machine learning was based on pattern matching to find information, which is simplistic for data with formats. However, advanced machine learning can correlate surrounding data, otherwise known as context, to increase the confidence score of accurate labelling.

Classifiers can be pre-built for commonly used identifiers in industries such as financial services, retail, or mining. However, many organisations have created bespoke data that require sensitivity monitoring and have utilised queries or scripts to find exact data. As stated, this is a time-consuming and manual process that can be avoided with AI-based data classification technology. Fine-tuning machine learning classifiers based on an organisation's data can greatly reduce the risk of human error and help organisations identify their most sensitive and critical data, thus proactively addressing privacy issues before they become an elevated risk.

Another significant benefit of AI modern technology is its ability to automate many of the manual tasks associated with data management, such as inventory, remediation and retention. An inventory is a collection of

data sets utilised by an organisation that also serves as common knowledge in an organisation. In the past, technology teams were tasked with documenting structured data in systems and data teams relied on the accuracy and completeness of the documents to track data usage and understand the context of the data. This information was used across different teams to either fix data issues or identify relevant data per each retention policy. For example, marketing teams would rely on business glossaries from technology teams to correctly pull data from a data warehouse to create a campaign list. Incomplete information in this inventory could lead to operational inefficiencies and delays in processing the data.

Remediation is a cross-functional activity with the technology and data teams that can be assisted with AI-discovery to help understand data domains with high probability of issues. Business teams are often responsible for identifying the business rules that monitor for data quality. Any significant changes to the acceptable thresholds for the data quality rule scores will trigger a workflow that will notify the proper personnel to review and correct the impacted data. Again, the traditional methods for identifying data for remediation is a defensive posture that relies on errors to occur before fixes are applied. However, there are proactive methods for identifying data to be remediated without incurring delays.

Lastly, retention management is also a difficult process for organisations to track and identify all the data files that pertain to each policy. AI-discovery can assist with automatically linking metadata to each policy and route for workflow action flows. Traditionally, this process required legal teams to write policies on the retention periods for each type of data that needs to be applied for each global region. This required technology teams to manually write queries to identify the relevant data tied to each policy. Auditors had difficulty tracking and monitoring the timeliness of each records management policy. However, this business use case can be easily identified and solved through AI-discovery that can continuously link together the retention policies to the metadata that tracks each data, irrespective of whether it is in a structured or unstructured format.

Real-time monitoring of enterprise assets

The benefit of modern technology is the accurate and timely responsiveness to data changes. AI data management can assist with privacy compliance and cyber security threats by providing organisations with real-time monitoring and reporting capabilities. These capabilities allow organisations to automatically track and analyse data usage patterns and detect any unusual or suspicious activity. The petabyte scale of data that enterprises must govern requires a new level of operational efficiency and monitoring. This requires automation at the very beginning of creating and collecting data assets to help organisations quickly identify and respond to potential privacy breaches and take steps to prevent them from happening again in the future. By leveraging AI, audit flows can be tracked and monitored for regulatory compliance, which is a critical piece of providing transparency to customers, executive boards and regulators. Full end-to-end compliance can be achieved through the use of data governance and data lineage tools, which can be used to track the flow of personal information within an organisation and provide a clear audit trail of all data usage. This can help organisations demonstrate to regulators and customers that they are taking privacy seriously and are committed to protecting personal information.

Natural language processing extends to data governance

In recent years, AI has been applied in data management through the use of natural language processing (NLP). NLP is a branch of AI that allows machines to understand and generate human language. This can be particularly useful for data management tasks for data scientists and data analysts that need to perform tasks such as text analysis and text mining.

Example: NLP algorithms can be used to automatically extract information from unstructured text data, such as customer reviews or social media posts, and to classify and categorise the data based on certain criteria.

The process of categorising data based on the discovery results is critical for businesses in order to take action on the findings of the AI-discovery process. In other words, AI can help discover and find information but technology has the ability to categorise data in different groupings for data teams to take action. For example, Netflix is the king of categorisation. It uses NLP to understand the search criteria of customers along with the behavioural data of movie selections. Netflix provides suggestions for new movies based on categories such as Korean thrillers or Western cowboy action. AI technology that provides this additional level of context is ultimately creating the value-driven results that business stakeholders need to demonstrate to the executive board.

Benefits for increasing privacy and cyber risk management

There is little doubt that the usage of AI in all its different forms is innovative and disruptive. When applied to data management and governance for privacy compliance and cyber security risk management it can also show potential for increasing the scalability and effectiveness of compliance.

There is no doubt that with the increasing amount of personal data being collected, stored and analysed by organisations of all sizes and across all industries, the importance of data security and privacy is becoming more critical. AI technologies can be used to analyse data in real-time, detect potential security breaches and take action to prevent them. These capabilities allow organisations to track and analyse data usage patterns and detect any unusual or suspicious activity. It is imperative that action be taken to prioritise and implement the governance framework and technologies to reduce and minimise privacy and cyber security risks.

About the authors

Lisa Fitzgerald
Partner
Lander & Rogers

Lisa Fitzgerald is a partner at law firm Lander & Rogers within the Corporate practice, and co-head of its Digital Economy practice. Lisa specialises in technology, AI, blockchain and digital assets, data protection, privacy, cyber, media, intellectual property and telecommunications. She advises on a range of regulatory, contractual and corporate matters, from cross-border transactions to intellectual property strategy, digital transformation projects, legal tech and data governance. Lisa's thought leadership includes coining the term 'splitchain' to help anchor blockchain use cases within a legal framework.

Former Associate to former High Court judge, the Hon. Kenneth Hayne AC KC, Lisa also served as Acting Chief Privacy Officer for a major bank, is a Fellow of the Governance Institute of Australia, a Councillor on its Victorian State Council, a member of the Media and Communications Committee of the Australia Law Council and the CEDA Business Dynamism and Competitiveness Advisory Committee. Lisa also served as Non-Executive Director of a global software company.

Broderick Smith
Senior Data Governance Advisor
Intalock

Broderick Smith is a senior data governance advisor at Intalock, and is an experienced management consultant specialising in information governance, digital transformation, and virtual chief information officer (CIO) services. Commencing his career in operations management where he owned and built technology companies specialising in systems integration and managed services, Broderick has spent the past 15 years in information management and cyber security.

Broderick's experience straddles the private and public sectors and includes specialised knowledge of governance and statutory requirements within highly regulated sectors. A strategic thinker, he successfully plans and executes digital transformation and discovery with a focus on the impact that future innovation will bring to Australian organisations. Broderick has overseen large scale systems design and integration projects and corporate change programs in many industries including finance, logistics, health care and not-for-profits.

Broderick offers in-depth insight into the organisational design of operational backbone architecture, digital platform design, shared customer insights and accountability frameworks that enable him to solve complex business problems while reducing risk and aligning a business' strategic objectives.

Broderick has a Bachelor of Engineering and a Masters in Technology Management from the University of New South Wales (UNSW), a qualification in Organisational Design from MIT Boston, is a certified blockchain and NFT expert, and holds numerous non-executive and advisory roles on boards including technology start-ups and a domestic violence not-for-profit.

Broderick is a CRN "Industry All-Star" for being in the CRN Fast50 for three consecutive years, and won the prestigious FinTech Industry Award for Innovation in 2017 for his insurance factoring platform. Broderick is a member of ISACA and FAIR and the International Association of Privacy Professionals.

Peggy Tsai
Chief Data Officer
BigID

Peggy Tsai is the Chief Data Officer at BigID, a data intelligence platform that leverages AI/ML to discover enterprise data for the purpose of privacy, security and data governance. She has over 18 years of practitioner experience in data management, stewardship and governance in the financial services industry.

Prior to joining BigID, Peggy was Vice President of Data & Analytics at Morgan Stanley where she helped run the data governance program across the Wealth Management division. She was the Data Innovation Lead in the Enterprise Data Management group at AIG. Peggy also worked at S&P Global Ratings where she held various positions in the Data CoE and Data Services.

Peggy has a Masters in Information Systems from New York University and a Bachelors of Arts in Economics from Cornell University. She is a founding member of the Women Leaders in Data & AI, as well as an advisor to several start-up companies.

Contributors