The New Governance of Data and Privacy:

Moving from Compliance to Performance

Malcolm Crompton

Michael Trovato

Contents

Foreword

As chair of the Australian Information Security Association (AISA) and director of Deakin's Centre for Cyber Security Research & Innovation (CSRI), I fully understand and appreciate the need for good privacy practices and strong cybersecurity in Australia at a government, industry and community level. It is important to acknowledge that board directors play a key role in shaping the culture and tone of organisations in these areas. Successful organisations have moved past compliance and towards building outcome-based resilience, increasing their ability to react, adapt or drive their markets forward before and after the unexpected happens.

In this publication, Malcolm Crompton and Michael Trovato share their considerable and unique perspectives from across industry and government and provide a valuable resource for directors to better understand the interactions between technology, business and regulation and how data should be thought of as both an asset and a liability. Managing data by focusing on the balance between performance and risk is critical and will result in achieving compliance as a by-product rather than via a tick-box activity. I believe this guide will help any director to understand some of the opportunities and challenges faced by their organisation, the mind-set they need and actions they should take. It will arm them with essential knowledge for the challenges that lie ahead.

Data and privacy governance is broad, deep and dynamic. As a result, directors will want to keep this publication handy, while increasing their knowledge through professional development and training offered by the Australian Institute of Company Directors and by staying alert to daily developments in this space. This is an exciting time for directors. They may not become privacy or cybersecurity 'experts' but they must develop the data and privacy literacy to be able to understand how to discharge their responsibilities and when to ask for expert advice.

I recommend this guide for boards, executives and regulators seeking to understand the new governance of data and privacy. It may challenge some of your current practices and preconceptions relating to management of data and privacy in a digitally-driven world, but I believe the benefits for your stakeholders will be immense.

Damien Manuel GAICD

Chairman

Australian Information Security Association

Preface

With the digitisation of everything, rising surveillance capitalism, intensive national security monitoring and large intelligence gathering activities, directors and boards worldwide have moved beyond seeing privacy as a compliance line item. As organisations endeavour to prosper, leading directors are asking themselves much more dynamic questions:

- Why do our customers and other stakeholders care about privacy and security?
- How can we increase organisational performance and innovate by using technology?
- What is the value of our data to our stakeholders and those that might do us, or society at large, harm?
- How do we protect our data? Are our business, risk, information technology (IT) and assurance functions engaged and providing reasonable performance and protection metrics?
- Are our actions ethical? If they became public knowledge, would we build or lose trust and social licence?
- Do we understand what it takes to be resilient and to be able to handle an unexpected breach?
- Do we have the right level of privacy and cybersecurity board literacy to make these judgements, while not placing reliance on executives or outside advisers?

These are difficult questions to answer, especially as many organisations have acquired a technology and risk debt in the form of legacy processes, systems and people, which groan and creak under the demands of a modern economy.

Our goal in writing this guide is to provide directors and boards with a good understanding of the privacy governance landscape that they face and the right questions to ask of their executives.

Although the technology may change, and new ideas for uses of data will abound, the following considerations should be addressed in board meetings to establish and maintain an organisational culture of sound privacy governance:

- How would we react to a serious data breach as a customer or other key stakeholder?
- Do we treat our data with the same respect we would any other major class of financial asset? How do we value it, invest in it and protect it?
- Have we discharged our privacy governance obligations as directors?

This guide is a valuable tool for directors and boards to help them think about and answer these questions, and we hope it will provide an understanding of the privacy landscape and how to increase organisational performance while meeting legal obligations and business requirements.

1. Introduction

We live in the age of the data deluge, where technology enables the supercharged collection and processing of data. Directors and boards are responsible for directing their entity to leverage data-driven opportunities while ensuring that privacy is built into its governance, control and management. To do less risks both loss of business opportunity and non-compliance with the law.

The following sections outline the opportunities and risks from both a compliance and performance perspective. Firstly, the guide provides an overview of the technological, business and regulatory developments that contribute to today's privacy landscape, including the extent to which they make data both an asset and a liability. Secondly, it covers key national, regional, and international privacy regimes, with a special emphasis on the European Union's General Data Protection Regulation (GDPR) and what it means for Australian organisations. Thirdly, it moves from compliance to performance, providing practical advice for directors and boards on establishing and overseeing privacy culture, frameworks and future-oriented practice. The guide concludes with ten key questions for directors to consider on the governance of data and privacy.

The principal theme that runs throughout this guide is 'focus on the customer'—their needs, expectations and interests. This is not an original insight. However, it bears repeating given the allure of new technologies, data sources and commercial interest to do more with more data. Fortunately, directors and boards don't need to rewrite the playbook. The key—as with all sustainable, long-term business success—is to focus on the customer.

1.1 Privacy: where technology, business and regulation come together

From a board perspective, it's useful to think of privacy at the intersection of three fields:

1. Technology. Tools and capabilities that facilitate or restrict the flow of personal information: that is, any information or an opinion about an identified individual or an individual who is reasonably identifiable. This guide will use 'personal information' and 'personal data' interchangeably; the terms have analogous meaning, with usage depending on the jurisdiction.[1]
2. Business. Strategies and decisions to leverage personal information for commercial gain in

[1] Note that both terms differ from 'personally identifiable information' (PII). PII originates from the legal context in the US and refers to specific pieces of information that can distinguish or trace an individual's identity, such as name, social security number, and date and place of birth. There have been instances where PII is conflated with personal information, both externally in the media as well as internally in Australian entities. It is important to recognise that personal information has a wider scope than PII as it applies to any information that could, alone or combined with other readily available information, reasonably identify an individual.

light of market conditions and opportunities.
3. Regulation. Formal rules that govern the proper handling of personal information.

All three fields—technology, business and regulation—have undergone dramatic changes in the last three decades.

In the late 1990s, innovations in Silicon Valley and the resulting market opportunity enabled Microsoft to achieve its (then) ambitious vision of "a computer on every desk". A whole new industry of software developers arose to build digital tools for word processing, data manipulation, video editing and much more. Software came in boxes and data remained relatively siloed in local storage.

After a false start, the internet era grew rapidly in the 2000s. Computers were linked together in local and global networks. Data could flow much more freely via open communication protocols. Connectivity allowed companies to reach customers and undertake new ventures. It led to the rise of the social web. It facilitated the rise of giants such as Apple, Amazon, Facebook and Google. Each leveraged the underlying dynamics of the internet—more web pages, more apps, more users and more information—to achieve dominance in their respective markets. Increasingly, companies and industries—from media and entertainment, to manufacturing and energy, to finance and communications—were being run on software and delivered as online services.

This growth of data flows led to greater personalisation. Companies were rewarded for offering better choice and services tailored to the individual preferences and needs of their customers. The salience and value of personal information increased; however, along with the benefits came attendant risks. Personal information could be used in ways unacceptable to the individuals concerned, as well as sought by unscrupulous companies and other illegitimate actors.

Regulations arose to uphold the rights of individuals and to correct for market failure around the proper handling and protection of personal information. In Australia, the *Privacy Act 1988* (Cth) (Privacy Act) was amended in 2001 to extend its coverage to the private sector. Other Commonwealth legislation affecting the handling of personal information in the public and private sectors has also evolved significantly (see **Part 4** for an overview). By and large, state and territory privacy legislation has less impact on the private sector except in regard to health service providers and contractors to government.

Technological advances accelerated in the 2010s. Connectivity extended from desktop and laptop computers to smaller mobile devices. With the smartphone revolution, we now carry the internet and gigabytes of data in our pockets. Cloud computing enables us to share and have enhanced access to apps and documents, while providing for increased storage—again, gigabytes at a time. More fundamentally, this period is characterised by the emergence of personal information as a new asset class.

Today, technology enables the supercharged collection and processing of data: the data deluge. On the collection side, our smartphones are king—recording every swipe, app interaction, photograph and GPS coordinate. In the digital world, every activity and transaction leaves a trail of metadata sometimes referred to as ‘digital bread crumbs’ or ‘digital exhaust’. Real-world data collection is enabled by the Internet of Things (IoT), the network of connected, sensor-equipped physical devices. IoT sensors are proliferating in every environment, including homes, factories, offices, farms, cities, rainforests and oceans. IoT data collection is becoming so fine-grained in certain contexts that the data can arguably be considered personal information.

On the processing side, more powerful and available computing resources allow incoming data to be analysed and used to derive value. The term ‘big data’ gained prominence in the early 2010s to refer to the processing of voluminous and complex datasets. Big data sets enable machine learning (ML), which refers to using statistical techniques on data to progressively improve a computer’s performance—that is, ‘learn’—on a specific task. ML is the underlying technology behind natural-language processing, image recognition and various forms of artificial intelligence (AI). In time, the application of big data and ML is likely to have profound effects on various industries, including transportation, healthcare, finance and more.

The changing technological landscape presents a challenge to the prevailing regulatory framework. Current privacy and data protection laws around the world can be traced back to the 1980 OECD Privacy Guidelines.[2] The Privacy Guidelines introduced several principles that have been widely adopted today, including collection limitation, purpose specification, use limitation, data quality and security, openness, and access and correction rights.

In today’s data deluge, however, some of these principles are under strain:

- Is the collection limitation outdated if the greatest business and societal benefits arise from maximising the data pool?
- Does it make sense to specify the purposes beforehand if the best ideas don’t exist until the data is collected and analysed?
- Is it wise to limit use to the original purposes if new, beneficial uses are yet to be discovered? What if it is impossible or impracticable to obtain each person’s consent for the new use?
- More broadly, what is ‘personal information’, given ever-increasing data collection and the prospects for re-identification?

What is not in doubt is the ramping up of public and governmental scrutiny of digital technology in general and data handling practices in particular. The rosy view of improving lives and connecting people has given way to a more sober reality as the consequences of the data deluge have unfolded. Data breaches and improper data handling practices are not only causing problems in the business domain

[2] Organisation for Economic Co-operation and Development (OECD), 1980, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 23 September, http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm, (accessed 19 July 2018).

but also in the private lives of individuals as well as more broadly for civil society, as vividly demonstrated by the Facebook-Cambridge Analytica data scandal.[3]

Directors and boards must be aware of these dynamics and consider privacy with fresh eyes. Privacy can no longer just be a compliance issue. The handling of personal information has financial, legal, strategic and risk implications. Of course, the situation is double-edged. The downside risks of data mismanagement are proportional to the upside potential of leveraging data for valuable ends.

[3] Wikipedia, 2018, *Facebook–Cambridge Analytica data scandal,* https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal, (accessed 19 July 2018).