CHAPTER 16:

Innovation in the regulatory environment

Data is an organisation's core business

Annelies Moens FAICD
Managing Director Privcore Pty Ltd

Why directors should take care

Data is an asset or a liability depending on how it is managed and in this sense, every organisation (business, government and not-for-profit) is a data business. As an asset or a liability, data is a core topic with which directors must make themselves comfortable and familiar.

Furthermore, a lot of data in organisations is about people, their lives, what they do, where they go, what they buy, what they like, what they say, what they look for, what they do for entertainment and so on – it is personal information and thus in many instances is subject to privacy and data protection requirements. Data is so integral to organisations, that it must be treated as core business. Data protection and privacy also has the added dimension of being considered a human right in some jurisdictions.

In order to lead successful organisations, boards need to develop a vision which enables their organisations to make decisions that build trust with their customers. Customer trust and customer privacy go hand in glove and the governance of data is not something that can be relegated effectively to compliance and IT functions without board oversight and direction.

Themes impacting the governance of data

Trust and social licence

The 2017 Edelman Trust Barometer reveals that trust is in crisis around the world. The general population's trust in all four key institutions — business, government, NGOs, and media — has declined significantly. Yet for innovation to flourish, trust is critical and innovation depends increasingly on the use and sharing of data.

In Australia, the Office of the *Australian Information Commissioner's Australian Community Attitudes to Privacy Survey 2017* shows that "in 2017, one in six (16 per cent) would avoid dealing with a government agency because of privacy concerns, whilst six in ten (58 per cent) would avoid dealing with a private company". Boards need to think about how their organisations communicate with stakeholders. How do they build and shape expectations with customers? It is certainly not shaped by the terms and conditions of products and services.

Mass customisation

The term 'mass customisation' refers to our present-day era where we have taken the handmade bespoke aspects of the pre-industrial era and the mass production capability of the industrial revolution era to be able to produce customised things at scale.

In our mass customisation era there is a need for customer centricity, where we need to understand our customers at an individual level in order to provide for their bespoke needs. Yet at the same time, ensuring an organisation has a 360 degree view of a customer is NOT a customer centric approach, as customers may not want to fully reveal themselves to organisations. Customers may want to be able to choose what they share.

Privacy is all about giving the customer control of what happens with their data – making them the driver and the reason for our products and services. As such, customer service and managing failure, including data breaches, are becoming increasingly critical touchpoints in determining the level of engagement and goodwill customers have towards brands and institutions.

Increasing number of data breaches

Being able to manage failure is increasingly important as more and more organisations are subjected to data breaches due to either their own inadequate security practices or system/human failures or unfortunate external attacks against which they cannot protect themselves.

The more data that leaves controlled and protected environments, the more we are polluting our data ecosystem. Identity fraud increases, trust diminishes (both ways between customers and organisations) and billions of dollars get wasted. Australia's focus on cybersecurity to ensure organisations have control of the data for which they are custodians is becoming increasingly critical.

Technology

Technology is rapidly dictating our policies as legislatures and policy makers struggle to keep up. We are in a world where it is easier to keep data than delete it and it is easier to create systems that retain data. More and more data will be collected about people as more devices become connected as the Internet of Things saturates our lives.

We have new technologies that are impacting massively the handling of individuals' personal information:

- Automated driverless cars and the collection of masses of data from sensors, voice and behaviour;
- Automated algorithmic decision making and artificial intelligence impacting our day-to-day lives;
- Social credit scoring;
- Biometrics and facial recognition in private and public spaces;
- Digital identity management;
- Cloud services through which data storage and processing is outsourced.

Whilst none of these technologies are inherently bad, they can rapidly lead to massive increased individual risk, through over collection of data, data breaches and misuse

or out of context use. These issues can be minimised with appropriate governance, which will be needed in order to retain customer trust.

What directors can do to build trust

Develop a culture of respect

The importance of culture cannot be underestimated. In an Independent Review of the Accident Compensation Corporation (ACC) in New Zealand, following a data breach that occurred in 2012, culture was the biggest transformational issue for ACC. It had had inconsistent practices around respecting personal information which led to numerous incidents around inappropriate handling of personal information. Today, New Zealand government agencies have privacy maturity assessment frameworks in place and a whole of government Chief Privacy Officer as a result of that Independent Review so that confidence and trust in New Zealand government can grow.

Make privacy part of risk management frameworks

According to the World Economic Forum's *2017 Global Risk Report*, alongside terrorism and extreme weather events, one of the top five risks facing organisations is massive incident of data fraud/theft. As such, privacy needs to be part of risk management and assurance processes.

Make leadership accountable

What gets measured gets done. If no person at senior executive level or board level is responsible for the decisions their organisation makes with respect to what happens to customer data, the direction the organisation takes will likely be dictated by factors other than core values such as respect for personal information.

Monitor key indicators such as input from customers, suppliers and employees

Listen not just to senior executives but also to customers, suppliers and a broad set of employees. Consider how fast bad news travels to the board and whether privacy is a regular board agenda item. How are failures and complaints managed within the organisation?

Collaborate with the regulator

Regulators with collaborative approaches, like the Office of the Australian Information Commissioner, tend to have more successful regulated outcomes (plus most complaints are negotiated settlements). The Office of the Privacy Commissioner in New Zealand is also innovative in its regulatory approach by introducing a Privacy Trustmark, whereby it is willing to indicate services or products that take data protection seriously and give customers confidence their personal information will be respected and protected.

Upcoming changes to privacy law in 2018

On 22 February 2018, the mandatory data breach reporting scheme came into operation and forms a new Part 3C to the Australian *Privacy Act 1988* (Cth). All breaches of regulated entities that are likely to cause serious harm to individuals will need to be notified to the affected individuals and to the Australian Information Commissioner.

On 25 May 2018, the General Data Protection Regulation in Europe will come into operation and include extra-territorial application to Australian organisations affecting European customers.

On 1 July 2018, the Australian Public Service Privacy Governance Code comes into operation, which Australian government agencies will need to abide by. The objectives of the Code are to:

a. set out specific requirements that agencies must undertake as part of their compliance with Australian Privacy Principle 1.2;
b. enhance the privacy capability and accountability of agencies;
c. promote good privacy governance within agencies to create and embed a culture that respects privacy and treats personal information as a valuable asset; and
d. build community trust and confidence in the personal information handling practices of agencies.