Customer consent and privacy

How to protect yourselves and your customers

June 2021
Introduction

Ask a CMO what their greatest risk is and you will hear about category disruption, delivering on the brand proposition, or attracting and retaining talent. Most do not realise there is a far greater risk lurking – how to use and store customer data.

Despite headlines citing penalties for brands, continued data breaches, and proposed privacy laws – most marketers and digital ambassadors remain blissfully myopic about their responsibility to manage customer privacy.

How did we get here? For the better part of a decade, marketers have been in a data arms race believing the more they knew about their customers, the better they could tailor experiences. In reality, only a handful of organisations in Australia are using this data effectively. The holy grail of personalisation and automation is still beyond the capability of most, and the data collection obsession has created unnecessary risk.

Consumers are growing wise to it too. Ninety-three percent now expect to opt-in to non-essential uses of their data rather than having to opt-out themselves. Poor use of data also influences their purchasing decisions, with 66% confirming they had backed out of a transaction or closed an online account over privacy concerns.

Marketing teams need to take urgent responsibility for customer data and the risk it poses to their organisation. Understanding your obligations around privacy, consent and data – and how each influences the other – is the first step.

But, this responsibility extends even further. Even if we are comfortable with our compliance today, change is accelerating – in both technology and the enforcement of regulations. Dynamic intelligence and a strong governance structure is critical to ensure you stay ahead of the curve and understand new risks as they unfold. After all, compliance is not a state an organisation reaches but a continued process.

---

Regulatory Landscape

Regulation has historically struggled to keep pace with emerging technology – but the tables are starting to turn. The past few years have been characterised by regulators clawing back the balance towards the protection of customer data.

As new legislation comes to the fore, marketers have an opportunity to improve compliance as well as marketing practices in the long run.

A quick history lesson

A key focus in global privacy law has been notice and consent. Whether express or implied, it is critical to understand what we need consent for and how we honour it in the background too. In Australia, the Privacy Act 1988 regulates consumer privacy, whilst the Spam Act 2003 establishes key rights and expectations regarding electronic marketing consent and opt out obligations for businesses.

Across the globe, many governments have introduced more robust privacy regulations aimed at enhancing consumer protections and individual rights. These regulations are backed by stronger investigation and enforcement powers to facilitate compliance.

- 26 November 2017: Australia introduces the Consumer Data Right (CDR), giving Australians access and control over their data. Initially focused on the banking industry, it will eventually roll out to other industries, beginning with the energy sector.
- 25 May 2018: The EU General Data Protection Regulation (GDPR) comes into effect to provide citizens with enhanced individual rights and harmonise regulations across Europe.
- 17 March 2018: The Cambridge Analytica scandal breaks.
- 21 January 2019: Google is fined €50 million by the French regulator over not properly disclosing how its data is collected and used in advertising.
- 8 July 2019: British Airways is fined €204.6 million by the UK Information Commissioners Office (ICO), the largest GDPR fine to date, for a breach that saw website users diverted to a fraudulent site.
- 24 July 2019: Facebook is fined a historic US$5 billion by the US Federal Trade Commission (FTC) for deceiving users about its ability to control the privacy of personal information.
- 1 January 2020: California introduces the Consumer Privacy Act (CCPA) providing enhanced rights for consumers.

---


5 https://secureprivacy.ai/gdpr-the-6-biggest-fines-enforced-by-regulators-so-far/

31 January 2020: Optus is fined $500,000 by the Australian Communications and Media Authority (ACMA) over significant breaches of the spam act through both text messages and emails.7

2 July 2020: Woolworths is fined more than $1 million by the ACMA after it discovers over 5 million breaches of the Spam Act 2003.8

16 August 2020: Brazil’s General Data Protection Law (LPDG) comes into effect.

1 December 2020: New Zealand’s Privacy Act 2020 comes into effect, including new requirements for cross-border transfers and mandatory data breach reporting.

Upcoming changes
With shifts happening around the globe, it is no surprise the Australian Government has plans to follow suit.

Already in the works are plans to tighten controls on the behaviour of key digital platforms as well as better protection for consumer privacy. On 30 October 2020, the Attorney-General’s Department released the terms of reference and issues paper for the Australian Government’s review of the Privacy Act 1988 (Cth). The review is considering a broad range of changes through a consultative process, with a discussion paper due for release in 2021. The issues paper largely follows the recommendations set out by the Australian Competition and Consumer Commission (ACCC) in the Digital Platforms Inquiry, released in July 2019.

The ACCC will also continue its ongoing inquiry into the operation of digital platforms in Australia, with further recommendations for sweeping legislative and policy reform likely to follow.

Further, the Office of the Australian Information Commissioner (OAIC) is taking Facebook to court over the Cambridge Analytica scandal, alleging contravention of Australian privacy law. The case is moving forward and has the potential to impact the future of consent and privacy in Australia.

8 https://www.afr.com/companies/media-and-marketing/woolworths-cops-1m-media-regulator-fine-over-spam-20200701-p5582g
How are you at risk today?

In a world where trust is in short supply, getting privacy, consent and data right is critical. The challenge for most marketers is that consumers are still willing to trade personal information if they see a benefit. Sixty-one percent of millennials are happy to share data if it leads to a more personalised in-store or online shopping experience.

This opportunity comes with a caveat – brands must meet customer expectations of privacy. If you fail to manage the risks to privacy properly, you could face the following damages:

1. **Reputation**
   With consumers placing more responsibility on organisations to protect their data, reputational damage is common after a breach. It’s not just personal data that is violated – consumers rightfully feel the trust they had with the organisation has been too.

2. **Revenue**
   Most data breaches will require organisations to pause some part of their operations as digital systems go offline, impacting the revenue of the business. Further, the loss of customer trust can directly affect sales. Negative publicity may also lead to a reduction in brand advocacy and trust, and have flow-on effects on revenue. COVID-19 has exacerbated these risks as organisations manage their operations remotely in the face of new and increasingly sophisticated cyber threats.

3. **Costs and fines**
   In 2020, the average cost of a data breach in Australia hit $3.35 million. As more organisations move their staff to remote working through COVID-19, 70% of respondents to IBM’s Cost of Data Breach report expect this to increase even further. This includes the costs of remediating deficient processes and technology, communicating and notifying those impacted by the breach, and detecting issues with the use of data forensics.

   Importantly, the intentional misuse of data is punished more heavily than accidental breaches, shown by the high fines Facebook encountered over the Cambridge Analytica scandal.

---

A shift in responsibility

Where marketing is at risk – The five areas to be aware of

There is more to privacy and consent than just managing unsubscribe lists or providing disclaimers. Data can reside in unexpected places.

Marketers are an important piece of the data privacy and security puzzle – they see brand safety with a unique lens in the business. While they are unlikely to become cybersecurity experts overnight, it is important that marketers understand what data is being captured, where it is being shared and how it is protected – particularly as compliance requirements grow. The role that marketeers can play in building in trust-by-design is incredibly valuable to broader organisational value of data and customers.

This requires a fundamental shift in mentality. Gone are the old days of capturing every piece of data possible. Today’s marketers will need to use information strategically to construct a better, more engaging customer experience – with an ever-present eye on risk.

Areas in an organisation where you can be at risk

So where might these risks be hiding?

- **Consent:** One of the biggest challenges companies face is gaining a single view of the customer – particularly when it comes to consent. Understanding who has provided consent, when they did and what they consented to is one of the foundations of strong privacy controls.

- **Data:** It is critical to have well-documented data stores, and processes to ensure it is used correctly. This includes both owned data and third party data. It is also important to know how that is received and shared, as well as your retention and access policies. Knowing the rules across the life cycle of data is critical as it pertains to compliance.

- **Marketing:** Understanding your analytics, campaign and personalisation tools, how data is captured and how it can be lawfully used is key to providing a personalised experience for customers.

- **Security:** Businesses need strong technology and security practices in place to ensure customer data is protected. This cannot remain static – these practices need to be reviewed at the same pace attackers are evolving.

- **Unstructured data:** There is an increasing amount of unstructured data being held by businesses including images and video as well as biometric data such as fingerprints or facial recognition. As it becomes the norm to offer fingerprint or facial login options, we need to pay careful attention to how that data is stored, used and protected given its high sensitivity.

Preference management and thoughtful marketing practices can help ensure customers navigate content they want and don’t want to interact with - without having to opt out completely.
## How to manage/what to do:

<table>
<thead>
<tr>
<th>Area</th>
<th>Typical risks</th>
<th>How to manage</th>
</tr>
</thead>
</table>
| Consent    | - Various consent lists  
- Agency owning distribution  
- Multiple unsubscribe options  
- No single view of customer  
- Existing consent options not in line with requirements  
- Third-party data sharing with limited understanding of privacy risks  
- Limited or no notice provided to an individual at the point of collection  
- Traceability of consent.                                                                 | - Build a single view of customer  
- Review all opt-out/unsubscribes  
- Store consent information including when the customer consented and what they consented to  
- Own all data, decision-making and delivery options  
- Align consent practices to your consent strategy and confirm you are honouring your promises to your customers. |
| Customer data | - Manual data processes  
- Low understanding of data stores and how third-party data is received and shared  
- Poor retention and access to policies or procedures  
- Poor data security.                                                                 | - Automated data processes  
- Updated data dictionary and single view of the customer  
- Strong security and data protections in place  
- Data handling training with employees  
- Strict retention and access policies and automation to support these  
- Cross-functional data steward officers. |
| Marketing  | - Non-compliant use of data for marketing purposes  
- Lack of understanding of all customer touchpoints and consent preferences  
- Complex marketing technology landscape with multiple tools in place (such as analytics, campaign and personalisation technology)  
- Low understanding of how data is captured, connected and can be used  
- An opt in or out process without email preferences, limiting customers’ ability to stay connected to relevant communications. | - Flexible and granular consent and preference management portal for customers  
- Marketing channel and preference communications planning  
- Simplified marketing technology platforms with reduction in extraneous or unintegrated platforms in use  
- Data privacy and process training for all staff. |
<table>
<thead>
<tr>
<th>Area</th>
<th>Typical risks</th>
<th>How to manage</th>
</tr>
</thead>
</table>
| Security           | - Ensuring stored or processed customer data is secure and protected  
- Cyber attacks  
- Human error that can cause security incidents or breaches.  
- Fines, cost and reputational damage done as the result of a breach.                                                                                                                                                                                                                       | - Strong technical security practices in place that aren’t static and evolve at the same pace as attackers  
- Data privacy and security training for all staff to understand the risks and the role they play in protecting customer data.                                                                                                                                                                                                                         |
| Unstructured data  | - Data that includes imagery, video and biometric data increasingly being stored by businesses  
- Often doesn’t trigger the same stringent processes that structured data goes through  
- Biometric data in particular is highly sensitive and used more and more for simple activities such as logging into an app.                                                                                                                                                                                                                             | - Unstructured data processes wrapped into wider data security and process protocol  
- Extra securities and processes in place for highly sensitive data  
- Data processes in planning or design stages of projects that involve capturing biometric data.                                                                                                                                                                                                                                         |
A practical approach

Today’s obligations and risks require a detailed understanding of how compliance wraps around people, processes, data and technology. This will not only safeguard you against today’s regulatory obligations but future shifts too.

When it comes to data security/privacy and consent & preference management, people, data, process and technology are intertwined.

When employees are well informed, it is one of the greatest assets in protecting organisation’s data. Leveraging and training talent to improve on ways of working, as well as capturing customer data in a consistent, reliable and transparent manner allows for efficiency between privacy and marketing processes. Moving forward, it is key to make privacy, consent and preference management a cultural focus of the organisation. If an organisation can get the change management components right, you are winning a key part of the battle.

In order for people to become well informed, it is important to design privacy into the processes that are used on a daily basis. This allows for a customer first approach to data collection and consent. These processes should be aligned to the organisations risk tolerance as well as business objectives.

Of particular importance is ensuring that consent is ‘meaningful’. Consent will be meaningful if it is voluntary, informed, expressly given, specific as to purpose, time-limited and able to be easily withdrawn.

Two-thirds of Australian consumers have indicated that they do not regard their consent to be valid when bundled with a broad terms of conditions and/or privacy policy. Moreover, 88% of consumers do not believe that their consent for non-essential uses should be enduring.

Once the processes are in place, it is time to select the technology. It is vital to evolve technology and monitor changes to it in order to deploy effective tools. The focus should be on centralised, secure, auditable and time-limited storage of customer data.

The foundations of consent & preference management

The right foundations of people, process and technology are critical for customer first and compliant consent and preference management.

Leveraging and training your existing talent to reshape default ways of working and drive improved consistency and reliability of customer data capture, not to mention more efficiency between privacy and marketing processes.

Evolving your technology and data architecture by focusing on centralised, secure, auditable and time-limited storage of data.

Transforming your business processes and governance by consistently designing privacy into the process and building a customer first approach to data collection and consent.

---

13 Deloitte Privacy Index 2020, pg7.
However, putting this into action can be a challenge.

We suggest focusing on the five areas of risk – consent, data, marketing, technology/security and unstructured data – and moving through them in a phased approach.

With each phase, you should take stock of your current situation, understand what you should be doing, and work out what needs to happen to bridge the gap. Breaking down this process is not only a more realistic option in today’s busy environment, but will give you time for a more comprehensive review.

It is important to recognise that while you should address each of these areas in isolation, there is a people and a process element underlying all data risk. Addressing this requires complete cooperation between sales and marketing, IT and data teams. It also includes risk, compliance and legal teams, who need to establish the right governance, procedures and systems, and ensure access to the right intelligence to monitor when the regulatory environment changes.

A natural tension may emerge between the teams who are mandated to address risk, and those wanting to maximise customer experience. Each organisation will manage this differently, but a solution is to have the customer experience principles and contact strategy agreed at the executive level. Another option is to embed privacy as a strategic pillar to drive advocacy within the organisation.

Specifically, by embedding transparent and privacy-centric design throughout its operations, an organisation can utilise privacy as an enabler to gain the trust of its customer base and maximise the utility of its data. Apple is leading this space by promoting its privacy principles and how these are baked into the design of its products and hardware.

It is also important to think about whether you want to take a customer centric or compliant-centric approach as that will shape the process. A customer-centric approach is focused on the experience and putting the customer first when thinking about data collection and management. A compliant approach is centred on ensuring the business is compliant with regulations as a priority, with the customer experience being secondary.

This value proposition will become more and more important in the future: demonstrate to customers that you respect their personal information (and by extension them) and you’ll be rewarded.
<table>
<thead>
<tr>
<th>Understand the regulations</th>
<th>What customer data do you have?</th>
<th>Review current state of 5 areas of risk</th>
<th>Design marketing and communication strategy with data privacy in mind</th>
<th>Implement marketing and communication practices in line with strategy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Establish the right approach for your organisation – one of compliance or one that is customer centric</td>
<td>How did you get it?</td>
<td>Consent</td>
<td>Update data stored if required, including capturing fresh consent</td>
<td>Implement necessary training and policies</td>
</tr>
<tr>
<td>How did you get it?</td>
<td>When did you get it?</td>
<td>Data</td>
<td>Integrate data to get to a single view of the customer</td>
<td>Implement data breach and request process</td>
</tr>
<tr>
<td>How can it be used?</td>
<td>Where are your gaps?</td>
<td>Marketing</td>
<td>Implement consent and preference management tools and automation</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Tech/Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unstructured</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Looking to the future

Today, your customers are increasingly digital savvy, aware of their privacy rights and suspicious of data collection. As concerns around privacy, data and consent grow, more regulation is likely.

It is still to be seen whether the Australian government introduces GDPR-like regulations on businesses. The Attorney-General’s Department is currently considering a range of potential reforms to the Privacy Act 1988, not limited to:

- Wider scope of what is considered personal information, including technical information
- Additional protections for de-identified information
- Removal of exemptions for employee records, small businesses, and political parties
- Increased enforcement powers for the OAIC
- Increased individual rights, including greater emphasis on consent and additional rights to erase personal information
- Greater harmony between the Privacy Act and other regulatory schemes.

The CDR will also be expanded to new industries over time, starting with the energy sector. While currently a requirement of the banking sector, this regime – which aims to easily provide consumers and third parties with data held on an individual – adds to the growing need for strong data storage management and processes, as well as a single view of the customer, to ensure that this process can be achieved easily. In addition, as regulation increases, so too does the importance of ensuring defined accountabilities for Privacy Officers and data owners responsible for managing compliance and establishing robust controls.

Equally, platform shifts towards more privacy-focused controls can disrupt the ability for marketers to make use of data. Moving forward, brands will need to better consider their marketing approach and move to more reliable sources of personalisation using owned data.

Whatever the future holds, you’ll need the right approach to privacy, data and consent. By working towards mature customer data management and governance, you’ll have a more sustainable approach moving forward. You’ll be able to accelerate faster, communicate better and build an experience your customers truly value. In doing so, you’ll turn your greatest risk into your greatest asset.