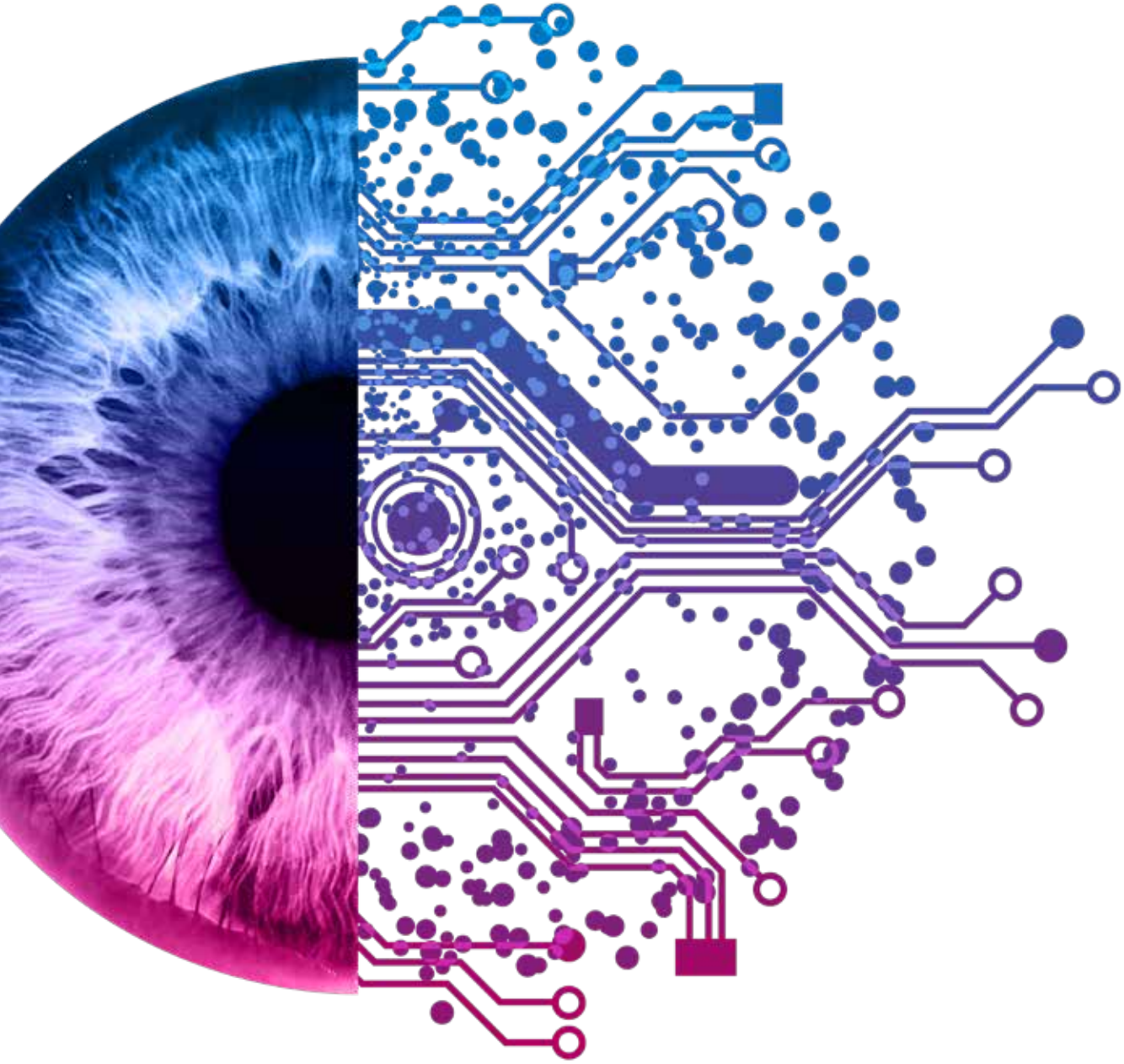


Allens › ‹ Linklaters

Risk e-business?

A guide to managing regulatory hurdles and adapting legal strategies as you accelerate your business online

DATA-DRIVEN BUSINESS

Over the past five years, growth in e-commerce has increased dramatically, significantly outpacing that of traditional retailing. The COVID-19 pandemic has further accelerated the consumer shift to online shopping. In 2019, there were 17.5 million users in the Australian online shopping marketplace. In under 12 months this number has surged to 18.3 million.

Data from Australia Post indicates that there was an 80% increase in online shopping between March and May 2020 and in April 2020 alone, more than 200,000 new shoppers entered the market and purchased something online for the first time. Seasoned online shoppers also notably increased their purchasing frequency.

This speaks to the high-level of market engagement and the emerging norm of shopping online. It has never been more critical for businesses to be able to engage and service their customers online and at scale.

This guide is designed as a legal roadmap for consumer facing businesses expanding their online offering.

Contents

Creating and expanding your online presence

Whether you are establishing an online presence for the first time or expanding your online operations after operating in the digital space for years, this section sets out some of the key issues to consider from a legal perspective when creating or refreshing your digital offering. Carefully considering your IT infrastructure, your relationships with suppliers and sellers and whether existing intellectual property protections are sufficient will create savings in the long run.

1 ARE YOU ACROSS YOUR IT INFRASTRUCTURE?

Your business' IT infrastructure is critical to the operation of your business – both online and in bricks and mortar storefronts. Understanding the IT infrastructure your business utilises and relies on – who provides it and owns it, how it is supported and maintained and where it is located – is important and a wide-range of stakeholders should hold this knowledge (not just 'the IT guy').

SECURITY AND THE CLOUD: A running theme through conducting business online is security, which should come as no surprise in an environment where threats evolve as quickly as they can be solved. As more and more business moves to the cloud, it is increasingly necessary for even non-technology professionals to have a good understanding of what the 'cloud' actually means, and the security risks involved in using it. In particular, ensure you understand who is responsible, and what contractual protections are in place, when something goes wrong.

OFF-THE-SHELF: Standard e-commerce solutions can be purchased off-the-shelf. If you choose to use an off-the-shelf solution, ensure you have the right licences in place for the current and anticipated scope and scale of your business. For example, ensure the licence covers the right countries and permits access for a sufficient number of users. Under-licensing can be costly to resolve. It is also important to check that the licence allows you to adapt or add to the software in future (eg incorporating additional functionality) as your business needs change.

OPEN SOURCE SOFTWARE: Open source software is software that is made freely available (usually over the internet) for anyone to use, change and distribute pursuant to a licence. If you decide to use and adapt open source software for your online business, ensure that you are aware of any potential restrictions or limitations placed on that software. For example, the licence for open source software often states that any adaptations made to the software will also be 'open source' (eg freely available to any future user).

CUSTOMISED SOFTWARE: If you commission a custom-built software solution or undertake customisation work on an existing product, ensure that you own the IP rights in the software or have a wide enough licence to give you freedom to use and modify it in the future. For example, confirm that the licence permits you to use third party contractors (as opposed to the original developer) to add new functionality to the system in the future.

BEWARE OF PATENTS – OR EMBRACE THEM! Clever ways of doing business online could potentially be protected by patents (eg Amazon obtained a patent for its 'One-Click' purchase feature). Ensure any terms agreed with a developer or supplier protect you against third party infringement claims. If you have developed your own unique system, consider whether it is eligible for patent protection.

ASKING THE RIGHT QUESTIONS

IT infrastructure

- When transitioning to the cloud or moving to a new cloud provider, ask:
  - what is being hosted on the cloud?
  - where are the servers located, including back-up and failover sites?
  - what is the scope of the cloud service?
  - what remains in the business' control or responsibility?
  - what happens when something goes wrong?
- Who owns the IP rights in your online platform or mobile app?
- Do you have adequate licences (if using a standard software product) and the right ownership / licence rights for any customisation?
- Have you thought about patent protection if you develop your own system?
- Do you have the appropriate permissions and licences to use and display the content you have on your website, including trade marks and logos?
- What is your business' position on the use of open source software?
- What is your business' position on making in-house developed code available as an open source resource?

2 WHAT IS THE STRUCTURE OF YOUR ONLINE BUSINESS?

The sales structure adopted for your online business can have important implications from an IP and competition and consumer law perspective. For example, many of the key legal considerations will depend on whether your online business structure is:

- more traditional, where you sell your own products or you are reselling products from suppliers; or
- akin to a marketplace where you are selling goods or services yourself but also hosting other sellers as well (eg similar to Amazon's structure).

RESELLER RELATIONSHIP WITH SUPPLIERS: If you are selling your own products or reselling products from suppliers, the IP and competition and consumer law issues that arise will be similar to those in a bricks and mortar context. For example, you need to avoid resale price maintenance issues, so you must set your prices, and your supplier shouldn't be trying to dictate or influence those. In addition, you will have primary responsibility for providing remedies under the consumer guarantees and you will need to ensure you have a compliant returns policy in place. From an IP perspective, as a reseller, you may be liable for the sale of any products that infringe third party IP rights.

MARKETPLACE WITH MULTIPLE SELLERS: In online marketplaces (such as Amazon), you may sell your own products and also provide a platform for sellers to sell direct to customers. This means you may be competing with your sellers. In this such casescase, to ensure cartel risks do not arise, you can set the price for your own products but you must never try to influence the price at which other sellers on your marketplace sell their products. This could raise serious price-fixing risks for you and your business.

FOR EXAMPLE, if you are going to sell in competition with sellers, like Amazon does, you need to make sure you don't have price-fixing issues.

Further, if you sell marketplace products as an agent for your suppliers, the primary responsibility for complying with the consumer guarantees, and offering remedies lies with the supplier as seller, rather than the agent. However, you must be cautious that you do not mislead customers about their consumer rights when acting as agent. In addition, you must comply with the consumer guarantees in respect of your own products. In formulating your complaints handling policies, you will need to create a process which complies with the consumer guarantees but you should also consider whether the process is simple and easy for your personnel to understand. Overly complex complaints handling procedures increase the risk of staff inadvertently breaching the consumer guarantees.

Marketplaces that sell third party products can also give rise to risks of additional liability if the third party product is IP-infringing. This risk varies by jurisdiction – there is no safe harbour protection for commercial marketplaces in Australia, and the degree of protection varies in overseas jurisdictions where it is available.

The risk level also depends on the specific terms of your arrangement with the supplier/seller (eg whether you are merely providing a listing of third party products, or if you are more actively involved in the supply chain, such as providing warehousing services or reselling the products yourself).

WHAT SHOULD YOU DO?

Structure of online business

- Determine how your online business will be structured from the outset (eg whether you will have a traditional relationship with suppliers as a reseller or intend to operate an online marketplace where you may compete with your sellers)
- Ensure that your pricing and complaints handling policies comply with competition and consumer laws, depending on the structure adopted
- Similarly, ensure that you address third party IP infringement risk appropriately, depending on the structure adopted. If adopting a traditional reseller relationship with sellers/suppliers, ensure your contractual arrangements with suppliers/sellers sufficiently indemnify your business from IP liability. If operating as a marketplace, implement an effective notice and takedown procedure to minimise liability for any infringement

3 WHAT PAYMENT PLATFORM IS YOUR BUSINESS USING ONLINE?

Your payment platform can make or break your customer's experience of your online business. Failure in the payment platform can mean a loss of sales – both in the immediate and long-term if customers lose trust or are frustrated by a poor experience. When choosing payment platforms, consider the security of the platform, availability of support and failover measures in place, and how many transactions the platform can handle. In addition, proactively plan for increases in demand – eg during a big sale or promotional event – to make sure you do not lose out in sales and customers are not disappointed.

WHAT SHOULD YOU DO?

Payment platform

- Ensure that you conduct due diligence prior to selecting your payment platform and have in place robust contractual protections with your payment platform provider that address liability in the event of a failure in a payment platform

Restrictions on suppliers

- Obtain competition law advice prior to including a 'most favoured nation' clause (or other restriction) in a contract with a supplier/seller
- Prepare a policy and implement competition law training for employees responsible for the commercial arrangements with suppliers/sellers to ensure they do not discuss or agree impermissible pricing restrictions

4 DO YOUR TERMS AND CONDITIONS WITH SELLERS/SUPPLIERS CONTAIN RESTRICTIONS?

Regardless of the structure of your business online, imposing restrictions on your suppliers or sellers can raise competition law concerns.

'Most favoured nation' clauses (clauses that require suppliers/sellers to provide their products/services on terms that are no less favourable than the best terms offered to any other retailer) have been subject to scrutiny by competition authorities globally, including the ACCC.

Competition regulators have found such terms to be anti-competitive in certain circumstances as they can create barriers to entry and soften competition by preventing competitors from negotiating better deals with suppliers . For example, in 2016, the ACCC investigated Booking.com and Expedia for their use of clauses requiring accommodation providers to offer best price and availability on their online accommodation platforms. The ACCC was concerned that this reduced price competition between competing accommodation platforms and also prevented consumers from negotiating a better deal direct with accommodation providers. Following the investigation, Booking.com and Expedia agreed to amend the price and availability parity clauses in their contracts.

Pricing restrictions and most favoured nation clauses can also raise cartel risks in certain circumstances, if your online business competes with your suppliers/sellers. For example, in 2018, travel agent Flight Centre was fined $12.5m for price fixing after it tried to persuade three airlines not to offer airfares on their websites that were less than those offered by Flight Centre.

ONLINE RESTRICTIONS | A GLOBAL EXAMPLE

The EU competition commission recently opened an investigation to assess whether Apple's rules for app developers on the distribution of apps violates competition rules. In particular, the commission will consider whether the following restrictions raise concerns:

- a requirement for app developers to use Apple's own in-app purchase system. Apple charges app developers a 30% commission on all subscription fees through that system; and
- restrictions on the ability of developers to inform users of alternative purchasing possibilities outside of apps (which are usually cheaper).

5 DO SOME OF YOUR SUPPLIERS / SELLERS COMPETE?

If you offer the products of two competing sellers/suppliers online, you must be careful what you discuss with each supplier/seller to avoid competition law issues.

For example, be careful not to inform one supplier/seller of the price negotiations occurring with a competing supplier/seller. Such behaviour may raise concerns that you are facilitating collusion between competitors by helping them to coordinate their commercial behaviour (also known as a hub and spoke cartel).

In 2013, the EU and US competition regulators investigated and launched proceedings against Apple and a number of leading book publishers alleging that the parties had engaged in price fixing.

In the US, the court found that the book publishers, with Apple's knowledge, together raised the prices of their eBooks, causing eBook prices to rise. The scheme arose in an effort to combat the downward pressure that had been placed on the price of eBooks as a result of Amazon's low price. Apple's subsequent appeals were dismissed, and it was ordered to pay a fine of US$450 million.

In the EU, the European Commission alleged a 'concerted practice aimed at raising retail prices of eBooks'. The publishers had entered into an agency model, allowing the publishers, rather than retailers, to set the prices of eBooks. The Commission stated that this coordination of commercial behaviour between the competitors, with Apple's assistance, was forbidden. In settling the dispute, Apple and four publishers terminated the agency arrangements, and committed to give retailers to the freedom to set their own prices for eBooks.

6 DO YOU INTEND TO SELF-PREFERENCE?

If you sell the products of suppliers/sellers online as well as your business' own products, your business should be aware of the risks of favouring your own products at the expense of the products of other sellers (known as 'self-preferencing conduct').

Self-preferencing conduct has come under scrutiny by regulators globally.

FOR EXAMPLE, in the EU, Google was fined for abusing its dominance by promoting its own shopping comparison service at the top of search results to the detriment of competing shopping comparison services.

The EU Commission is also investigating whether Amazon has taken advantage of its dual role as marketplace host and retail business to get exclusive access to competitively sensitive data from independent retailers to enhance its own offerings and sales, which could in turn harm competition.

Self-preferencing conduct can also raise consumer law issues. In January 2020, the Federal Court found that Trivago misled consumers by representing that its hotel aggregator website would help identify the cheapest hotel rates available. However, Trivago's algorithm actually placed significant weight on the fee paid to Trivago for each listing. As a result, more expensive room rates were often placed in a higher position than lower priced offers. The Federal Court has yet to determine a penalty for this.

WHAT SHOULD YOU DO?

Discussions with suppliers/sellers

- Ensure relevant employees are aware that suppliers/sellers may be competitors and provide guidance (eg training, policies) to relevant employees regarding their competition law obligations

Self-preferencing

- If you are considering promoting your own business' products above the products of other suppliers/sellers, seek competition and consumer law advice
- Ensure statements you make about offerings accurately reflect the way your business' algorithm works

7 DOES YOUR EXISTING BRANDING HAVE THE NECESSARY REACH AND DOES IT PROJECT THE RIGHT IMAGE?

As your business pivots and experiments with new offerings, it is important to consider whether you are adequately protected by your existing trade mark registrations for any new or expanded products or services you introduce. Many businesses are also innovating with their branding and marketing messages.

CLEARANCE SEARCHES: Before expanding the scope of your existing brand, or adopting a new brand for your new offerings, you should undertake IP clearance searches so that you can properly assess the risk that you may be in conflict with existing third party IP rights.

REVIEW YOUR PORTFOLIO: Moving or expanding online often presents a good opportunity to undertake a strategic review of your trade mark portfolio to ensure it aligns with your current business priorities and budget. Filing new trade mark applications can help you to stake your rights to your brand in new jurisdictions and protect you for your new products and services. You may also need to register new domain names and business names. The upfront costs need to be managed carefully, but may help you achieve significant savings when it comes to enforcement.

8 HAVE YOU DONE YOUR IP DUE DILIGENCE?

Operating in the digital sphere brings new challenges for ensuring that your products and services do not infringe third party rights.

NEW CUSTOMERS: Online businesses have the potential to attract new customers from different jurisdictions. Even if you are not actively targeting them, by operating in a global market you may need to expand your usual clearance and freedom to operate searches to check for potential conflicts with third party trade marks, designs and patents outside of Australia.

THIRD PARTY IP: If your goods or services use IP sourced from a third party, ensure that you either own the rights, or have a wide enough licence, to use them in the digital sphere and in all relevant jurisdictions. Some IP that is in the public domain in Australia might still be protected overseas.

FOR EXAMPLE, many early 20th century furniture designs that are not protected by copyright in Australia have recently gone back into copyright in the UK.

WEBSITE CONTENT: As the reach and traffic to your website increases, any infringing or unlicensed content is more likely to be detected. You should maintain comprehensive records so that, if challenged, you can establish that your content is original. Anything appearing on your website which you did not create yourself must be appropriately licenced.

WHAT SHOULD YOU DO?

IP protection

- If you are using a new brand or expanding into new territories or online offering, consider filing new trade mark registrations, as well as domain names and business names. Look for savings within your existing portfolio
- Consider undertaking a review of your trade mark portfolio to ensure it aligns with your current business priorities and budget
- If your platform is likely to reach customers in new jurisdictions, consider undertaking clearance / freedom to operate searches to cover these jurisdictions
- Ensure you have the rights to use any IP sourced from third parties in the digital sphere and in the right jurisdictions
- Ensure that the content of your website or app does not contain any unlicensed or unauthorised material

Managing customer data

Data is one of our economy's most valuable assets. It is transforming how organisations operate and how they deliver products and services to consumers. Personal information is often the most valuable type of data your business will have – and it is highly regulated.

1 IS YOUR DATA SECURE?

A key benefit to expanding your online business is the opportunities it presents in terms of collection of customer data that can be used to enhance your product offerings and services. However, with greater data comes greater responsibility.

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

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

When considering security of data for your business, also consider whether there are any specific regulatory obligations. For example, the Privacy Act requires businesses to take reasonable steps to protect personal information from misuse, interference and loss and from unauthorised access, modification and disclosure and the Payment Card Industry Data Security Standard sets out requirements for securing payment card information.

An important aspect to managing data, including its security, is to have in place an appropriate data governance framework which can identify potential risk areas, and mitigate those risks, by:

- identifying what data your business holds and the relevant data flows;
- embedding legal and regulatory compliance; and
- implementing controls over data handling and use decisions.

WHAT SHOULD YOU DO?

Data security

- Security of data is fundamental to protecting the value of data and mitigating risks of financial, regulatory and reputational risk. Consider practical measures to secure data, such as:
  - appropriate technological access controls (eg, passwords, etc);
  - understanding where data is stored at rest and assessing the suitability of that storage (including location, access controls, back-up procedures, etc);
  - having in place proper retention and destruction policies to ensure only data that must be retained or is actually useful is kept; and
  - taking out cyber risk insurance for when, not if, a cyber security incident occurs
- Put in place a data governance framework to inform your data strategy

2 ARE YOU USING DATA ANALYTICS?

As your business increases its online presence and collects more data, data analytics will become a more effective tool, assisting you to deliver better products and services and an enhanced customer experience.

New tools and methods allow for the collation of data from a wide variety of sources and reveal insights not previously possible. This can identify new opportunities for your business.

There are regulatory considerations when undertaking data analytics, especially in light of recommendations of the ACCC's Digital Platforms Inquiry .

Relevantly, the ACCC recommended that there be consideration as to whether the Privacy Act should offer protections for inferred information (ie the use of data analytics based on personal information to infer additional information about an individual) and de-identified information. If adopted, this could challenge the current business model of many organisations that avoid privacy legislation through the use of de-identified data or data that is not sufficiently linked to an identifiable individual.

WHAT SHOULD YOU DO?

Data analytics

- Wherever possible, use de-identified data to undertake analytics to minimise the risk of breaching the Privacy Act and embed good privacy practices into every step of the data analytics process

Data commercialisation

- When commercialising customer data, ensure that you understand regulatory implications, potential restrictions or limitations on the use of that data as well as any other fees that may be applicable

3 ARE YOU INTENDING TO COMMERCIALISE CUSTOMER DATA COLLECTED ONLINE?

The data your business holds offers significant value both to you and other businesses. Understanding that value, particularly how to leverage it, is not always straight-forward.

Remember that no one 'owns' data – neither businesses nor individuals. However, businesses and individuals may have rights to access, control and use data.

If you are considering commercialising any data you hold, eg through granting licences to a data set, it is important you consider:

- any regulatory limitations (eg, if any of the data is personal information, the Privacy Act will apply);
- how and to what extent access to data is granted;
- for what purposes the data can be used, and any limitations or restrictions on use; and
- the fees or other consideration that are applicable.

CALIFORNIA CONSUMER PRIVACY ACT

From 1 January 2020, California residents have the right to understand the types of businesses to whom their data has been sold and require a business to stop selling that data to third parties. Businesses subject to this Act must give consumers the ability to opt-out of the sale of their personal information. California is often on the forefront of privacy law, and this is the first law of its kind.

4 HAVE YOU CONSIDERED WHICH GLOBAL PRIVACY LAWS MAY APPLY?

While increasing your online presence can increase your business, it can also mean you are reaching markets you had not previously had access to and, as a result, collecting personal information from individuals located around the world.

It is important to understand which privacy laws apply, particularly as some have extraterritorial effect.

In addition to the Privacy Act, you might have obligations under:

- the EU General Data Protection Regulation (***GDPR***), even if you are not (and are not related to) a business established in the EU; and
- the California Consumer Privacy Act (***CCPA***) if you conduct business in California.

GDPR TRIGGERS: If you are not sure whether the GDPR applies to your business, consider whether you offer goods and services to individuals located in the EU and collect personal information about those individuals, or monitor individuals in the EU. Factors that point to you 'offering' goods and services to individuals in the EU, or monitoring such individuals, include:

- marketing directly to EU residents;
- accepting payment in Euros;
- making your website available in European languages (eg Italian, German, etc); and
- monitoring the use of your website and other digital channels through cookies, tracking, retargeting and the collection of IP addresses.

CCPA TRIGGERS: Your business may be subject to the CCPA if it does business in California and collects personal information of California residents, and your business meets at least one of the following thresholds:

- has an annual gross revenue in excess of US$25 million (it is unclear if this is global or only in relation to revenue derived in California, however until this is clearer it is best to err on the side of considering global revenue); or
- obtains personal information of more than 50,000 California residents, households or devices annually; or
- derives 50% or more of its annual revenue from selling, renting, releasing, disclosing, making available, transferring or otherwise communicating California residents' personal information for monetary or other valuable consideration.

WHAT SHOULD YOU DO?

Privacy laws

- Understand which privacy laws apply – if you are reaching a global market, you may be subject to non-Australian privacy laws
- Make sure you collect, hold, use and disclose personal information in accordance with any privacy laws that apply, including the Australian Privacy Principles under the Privacy Act
- Remember that personal information might be valuable data, but you do not 'own' that data and need to use and disclose it, including for analytics, in accordance with applicable law

5 ARE YOU ADEQUATELY DISCLOSING TO CONSUMERS HOW YOU WILL COLLECT AND USE THEIR DATA?

It is important that you are transparent with customers about how data collected through your online platform or website will be used.

FOR EXAMPLE, the ACCC recently commenced proceedings alleging misleading or deceptive conduct against both Google and HealthEngine in relation to their data practices.

WHAT SHOULD YOU DO?

Data Disclosure

- Be clear with consumers about how their data is being used, particularly if that data is being provided to third parties or for purposes such as advertising
- Consumers should be given the opportunity to make an informed choice as to whether to explicitly opt out from the collection and use of their data

SHARING DATA WITH THIRD PARTIES

The ACCC has taken action against online health booking platform, HealthEngine, alleging misleading or deceptive conduct relating to the sharing of consumer information with insurance brokers.

According to the ACCC, HealthEngine gave information such as names, phone numbers, email addresses and dates of birth of over 135,000 patients to private health insurance brokers for a fee without adequately disclosing to consumers it would do so.

DISCLOSURE REGARDING USE OF CONSUMER DATA

The ACCC has commenced two proceedings against Google. The first proceeding Google relates to two Google Account settings: 'Location History' and 'Web & App Activity', which enable users to control whether Google obtains, keeps and uses personal data relating to their location when they use Google services. To stop Google collecting and retaining location data, both settings had to be switched off. However, at certain times, the ACCC alleges that Google misled consumers by not properly disclosing this. The Commission also claims Google failed to disclose to users that it may use the location data for its own purposes, including for advertising. In essence, the ACCC claimed that consumers were deprived of the ability to make an informed choice about the collection and use of their personal location data, and that Google misled consumers. Google is defending the proceedings. This case is a reminder to communicate clearly with customers about the use of their data, and to address any potential or actual risks of inadequate disclosure.

The second ACCC proceeding concerns a change in Google's policy that expanded the ways in which Google would collect, combine and use consumer data, including targeted advertising. The ACCC alleges Google misled consumers when it failed to properly inform consumers and obtain their consent before it started to combine personal information in consumers' Google accounts with information about those individuals' activities on non-Google sites that used Google technology to display ads. In particular, the ACCC has stated that:

- The pop-up notification requiring users to consent to the policy change was misleading as consumers could not have properly understood how their data would subsequently be used.
- Google's earlier statement that it would 'not reduce consumers' rights without [users'] explicit consent' was misleading as Google did not obtain 'explicit consent' when it made the changes to its policy.

Connecting with your customers online

A significant benefit of having an online presence is the ability to connect with customers in new and innovative ways. With increasing regulatory scrutiny of conduct in the digital world, it is important that you understand your consumer and privacy law obligations when marketing to your customers online.

1 WILL YOU BE USING TARGETED MARKETING TO CONNECT WITH CUSTOMERS?

While targeted marketing online can be a great way to engage with existing customers and reach potential customers, it is important you understand how the targeting will occur, particularly as this almost always involves the use of personal information. Targeted marketing that falls outside of the Spam Act (such as Facebook ads, tailored banner ads, and in-app marketing) must comply with the Privacy Act. General campaigns across digital channels (eg where no personal information is used to target specific types of customer) is not so regulated.

APPLE CHANGES THE IIDENTIFIER FOR ADVERTISERS: Apple is changing how its identifier for advertisers (IDFA) (used to track a users behaviour across apps and websites when using an Apple device) works – users will now be asked to opt-in and will be warned when a business is trying to track them across apps and websites. Other mobile device OS platforms may follow suit. These developments will make targeted marketing that relies on user profiles built from IDFA data more difficult and will narrow the pool of customers to whom it applies. Familiarise yourself with any changes that may need to be made to your marketing strategy to ensure compliance with any Apple terms (eg you do not want your app pulled from the Apple app store for a breach of Apple's terms of use). It may also be prudent to revisit marketing strategies and consider whether they will still provide benefit under the new IDFA regime.

DIGITAL PLATFORMS INQUIRY: The final report in the ACCC's Digital Platforms Inquiry recommended that organisations be required to obtain a separate consent to collect, use or disclose personal information for targeted advertising purposes, which could not be made a requirement (ie a 'take it or leave it') of providing the service. The Government is undergoing consultation to identify what measures could be taken to implement this recommendation.

WHAT SHOULD YOU DO?

Targeted marketing

- Ensure that any direct marketing complies with the Spam Act and the Privacy Act
- Be cautious when using personal information to target marketing to individuals, including when targeting ads or offers to customers via Facebook ads or through in-app means (even if that app is your business' app)
- Understand what data sources your marketing campaigns rely on and how changes to those data sources (such as a move to an opt-in from an opt-out) can impact on your campaigns

2 IS YOUR ELECTRONIC MARKETING SPAM ACT COMPLIANT?

It is important to maintain proper records of consent to electronic marketing (eg via email or SMS) and to never send electronic marketing to anyone who has opted-out of marketing. Further, unlike the Privacy Act (which only applies to individuals), the Spam Act regulates all electronic messages, including those sent to businesses.

Any marketing that is to occur via email or SMS will be subject to the Spam Act. The Spam Act defines marketing very broadly and includes an electronic message that:

- advertises, promotes or offers to supply goods or services; or
- advertises or promotes a supplier, or prospective supplier, of goods or services.

FOR EXAMPLE, you may want to let customers know about your new app by sending an SMS message to customers. This may be helpful information, but it is likely to be considered marketing as it can be seen as promoting a service (the app) and/or promoting your business. As such, it should only be sent to customers who have not opted out of such marketing.

3 WILL YOU BE CONDUCTING PROMOTIONS ONLINE?

It is important to ensure that savings on products are accurately displayed and do not mislead consumers.

FOR EXAMPLE, in July 2020, the Federal Court found that Kogan had made false or misleading representations about a 10% discount promotion online because it had increased the prices of over 600 products immediately before the promotion. After the promotion ended, Kogan reduced prices, many back to pre-promotion prices. The Federal Court has yet to determine penalty.

When advertising a promotional price for a product or service, it is also important that you or the seller (as the case may be) has sufficient stock of that product. It is illegal for businesses to promote a product that is not available in reasonable quantities or for a reasonable period of time having regard to the advertisement (this is also known as bait advertising).

WHAT SHOULD YOU DO?

Spam Act compliance

- Obtain and maintain a list of consents to marketing and maintain a list of opt-outs
- Wash all marketing campaigns against the opt-out list
- Make sure that any important factual information (for example, operating changes in response to lockdown measures) is conveyed in a manner that does not blur the line into marketing. This requires considering the wording, context, presentation and any hyperlinks in the message

Online promotions

- If making savings representations, ensure it is a genuine saving. This genuinely requires that you have sold the products at the higher price for a reasonable period of time immediately before the promotion price
- Ensure that you (or your sellers) have sufficient stock for forecast sales during a promotion

4 WILL YOU BE USING AI TO SET PRICES?

Businesses are increasingly using sophisticated algorithms which incorporate market data to set prices. While this technology is useful, price tracking and price setting software may give rise to cartel or concerted practices risks in some circumstances.

In 2017, ACCC Chairman Rod Sims stated: 'In Australia, we take the view that you cannot avoid liability by saying "my robot did it".'

WHAT SHOULD YOU DO?

AI pricing

- If using AI to set pricing, provide competition law training to those adopting and programming such technology
- Monitor the effect of any automated decision-making to ensure it is competition law compliant

User generated content

- Be aware of the risks associated with processing or publishing user-generated content
- Make sure you have a policy in place that establishes clear standards about the content that your employees and third parties can post on your website or social media pages, and monitor compliance with the policy
- Consider what tools you will use to hide or moderate third party comments before they appear on your website or social media pages. Failing to remove defamatory content once you are made aware of it also exposes you to risk
- Implement processes for promptly removing comments, or other content, from your social media pages where they breach the platform's rules or contain potentially defamatory material

5 WILL YOUR ONLINE BUSINESS CONTAIN USER GENERATED CONTENT?

If your online business involves dealing with material provided by users (eg a service which prints user-uploaded photos), you may be exposed to liability if the material (or your reproduction of it) infringes copyright or other IP. The risk is higher if your platform makes user-uploaded content publicly available.

'Safe harbour' regimes in some jurisdictions may protect you from liability if you implement adequate procedures to remove copyright-infringing UGC once you become aware of it. It is important to note, however:

- in Australia, most e-commerce platforms are not covered by the copyright safe harbour regime (which only covers infrastructure operators, ISPs and certain non-commercial sectors); and
- some safe harbour regimes require a degree of proactive monitoring (such as under the EU Copyright Directive).

You should also be aware of the defamation risks that arise from content that appears on your website or any of your social media pages. You can be held liable as the publisher of that material even if it is posted by a customer or competitor, and potentially face a significant damages claim. You could also be exposed to a claim for misleading or deceptive conduct under the Australian Consumer Law.

AI TO SET POSTER PRICES

Following an investigation by the UK competition authority, two competing online sellers, GB Posters and Trod, admitted to reaching a prohibited agreement not to undercut each other's prices for posters and frames sold on Amazon. The agreement was implemented by using automated repricing software which the parties each configured to give effect to the cartel. The software enabled the sellers to adjust the prices of their products in response to the live prices of competitors' products, based on rules that were determined by them.

6 WILL YOUR WEBSITE PUBLISH CUSTOMER REVIEWS?

The ACCC has taken action in recent years against businesses that have published false consumer testimonies or reviews.

If your website displays customer reviews, there is a risk that suppliers/sellers may write false reviews about their products or may incentivise customers or third parties to write false reviews, both positive and negative.

As fake reviews can skew ratings, they are capable of giving consumers a misleading impression about the product. In 2017, the Federal Court found that Meriton had engaged in misleading or deceptive conduct in relation to reviews of its properties on TripAdvisor. Meriton had tried to prevent guests it suspected would give an unfavourable review from receiving emails requesting a review from TripAdvisor. It did this by either not sending the email addresses of those customers to TripAdvisor or by inserting additional letters into those customers email addresses so that the prompt from TripAdvisor would never be received. The court found that this was likely to mislead consumers as to the nature, characteristics and suitability of its accommodation services. Meriton was ordered to pay a penalty of $3 million.

Your moderation mechanism for customer reviews may also need to look out for defamatory material and material that infringes third party copyright or other IP.

7 ARE YOU PROTECTED AGAINST DIGITAL INFRINGEMENT?

Increased online presence can lead to an increase in the risk of digital infringement. The World Intellectual Property Organisation (WIPO) has reported a surge in cybersquatting during the COVID-19 crisis. Squatters may register your business name or brand in different domains (and ask you to buy the name for money), or register similar domain names to attract traffic intended for your platform. The wide range of available general domains presents increased opportunities for squatters.

Other infringers are copying the branding and look and feel of legitimate platforms, capitalising on the business' reputation and taking advantage of unsuspecting consumers. The rise in online trading has also led to an increase in counterfeit goods, particularly pharmaceutical and healthcare products.

Enforcement in the digital world requires innovative strategies that combine a number of enforcement tools. These can include:

- joining the brand protection programs offered by global platforms and marketplaces;
- educating consumers and providing reporting tools to help identify infringements; and/or
- customs records in key markets for counterfeiting.

WHAT SHOULD YOU DO?

Customer reviews

- Ensure suppliers/sellers understand what can/cannot be done from a consumer law perspective in relation to customer reviews
- Incorporate your expectations and requirements regarding customer reviews into your agreement with suppliers/sellers
- Monitor reviews to reduce the risk of misleading or defamatory content and IP-infringing material being advertised on your website

Digital infringement

- Update your IP monitoring and enforcement strategy to protect against cybersquatting and digital infringement

Your workforce online

Accelerating digital customer engagement can open up new opportunities for managing and structuring your workforce. Alternative and adaptable workforce models can be used effectively – provided risks are well managed.

1 WHAT ARE THE KEY RISKS IN MANAGING AGILE WORKFORCES?

Contingent workforce models that make use of contractor or labour hire arrangements can allow your business to adequately scale to customer demand in the digital environment.

But what key risks need to be managed?

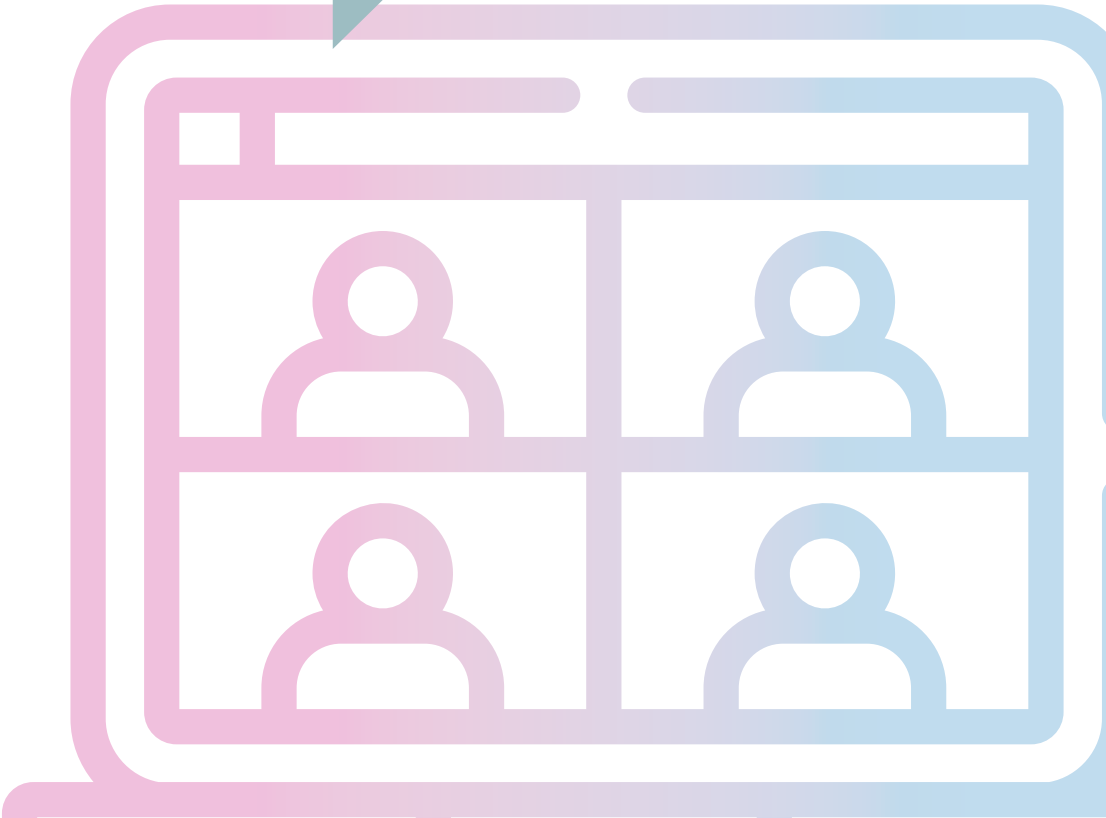
SUBSTANCE OVER FORM: whether a worker is an employee or independent contractor will be assessed by looking at the totality of the relationship – not just the words of the relevant contract. Managers and other people leaders should be aware of this and ensure they are using the right kinds of labour in the right ways. Agile or contingent workforces should be used only where the intention genuinely is for a non-permanent, non-employee engagement.

LICENSING AND SUPERANNUATION: even where your business is using genuine labour hire or contractor arrangements, be mindful that there will still be a regulatory overlay. In particular, many Australian jurisdictions impose labour hire licensing requirements on recipients of labour hire services and some independent contractors are entitled to superannuation contributions.

WHAT SHOULD YOU DO?

Relationship with your workforce

- Consider the relationship you wish to have with your workers or employees and ensure your contracting practices reflect that intention
- Should your business wish to use labour hire or contractor arrangements, ensure you are aware of the regulatory overlay and any obligations imposed on you (eg in relation to superannuation contributions)



2 HOW WILL YOU MANAGE YOUR SAFETY OBLIGATIONS FOR AN ONLINE WORKFORCE?

Regardless of whether your workforce is employee or non-employee based, your business will have work health and safety (WHS) obligations in respect of those workers. What are some key safety concerns in a largely digital environment where workers are often working away from a centralised location?

A WORKPLACE IS A WORKPLACE: your business' WHS obligations extend to your workers' remote, decentralised and digital workplaces. Your business must take reasonably practicable steps to ensure those workplaces (which might include your workers' homes) are safe.

MENTAL HEALTH: businesses increasingly appreciate that mental health risks, illnesses and injuries are as much a safety issue as physical injuries. Businesses' WHS risk management in the digital environment should acknowledge this and businesses should identify reasonably practicable steps that can be taken to eliminate (or mitigate) those risks.

WHAT SHOULD YOU DO?

Safety

- Understand that your WHS obligations extend to digital or remoter workplaces and take reasonably practicable steps to ensure that those workplaces are safe. This may include extending WHS practices to cover mental health risks

3 HOW WILL YOU MANAGE YOUR BUSINESS' ONLINE REPUTATION?

The more your business accelerates digital customer engagement, the greater the value of your business' digital presence and reputation and the greater the risk presented by one of your worker's ill-judged or improper social media posts. As many businesses have discovered, one worker with a social media account and a smartphone can inflict significant reputational damage.

Forward planning is key to managing many of these issues.

Consider, in particular whether your employment contracts and workplace policies:

- contain provisions that will enable to you exercise appropriate control over workers' social media use – in particular social media use where there is a connection to your business;
- help to delineate between 'business' and 'personal' social media accounts;
- provide for a clear understanding as to who 'owns' the 'business' social media accounts; and
- contain suitably robust post-employment obligations regarding non-disparagement and confidentiality.

ASKING THE RIGHT QUESTIONS

Your online reputation

- Do your employment contracts and contractor agreements contain provisions that deal with social media use, disparagement or other conduct that damages the reputation of the business? Do these agreements provide your business with the right mechanisms to respond to a worker's damaging social media activity?
- Are workers given clear direction about the extent to which (and how) their 'personal' social media presence can be distinguished from online activity as a representative of your business?
- Do your agreements with workers make clear who 'owns' social media accounts that are used for business purposes?

Digital transformation

Robust, resilient and of-the-minute technology is key to being successful online. Ensure that you are prepared for digital transformation by putting in place frameworks that enable your business to be agile and flexible when it comes to technology upgrades in the future.

1 ARE YOU PREPARED FOR DIGITAL TRANSFORMATION?

Digital transformation is arguably the most important board agenda as businesses race to adapt to new expectations from customers, and to change the way that work is done across the business.

The pandemic has driven the acceleration of digital transformation and the immediate need for change in how business and commerce is provided. With greater focus on online delivery of services and products led by the expectation of customers, businesses across every sector are faced with rethinking their engagement, delivery and logistics models.

In this context, spending on issues that are critical to an organisation's customer value proposition (such as technology transformation and digitalisation) or survival will be considered essential.

WHAT SHOULD YOU DO?

Preparing for Digital Transformation

- Consider areas where you can afford to take some risks (eg adding a new feature to your app) and where you need to be more cautious (like your critical IT infrastructure and how customer information is used or stored)
- Understand that reliable technology is critical to being a successful business and it pays to invest in current and future technology
- Use technology roadmaps as a tool for planning and strategising both the short-term and long-term changes in your business' technology environment

TECHNOLOGY ROADMAPS: A TOOL FOR THE FUTURE

A technology roadmap is a high-level plan that supports planning, strategising and communicating what, when, why and how certain technologies will be onboarded (including identifying when some technologies will be reaching end-of-life). The technology roadmap can be used to align key stakeholders across business units by creating a clear action plan around technology, having regard to the overall objectives of the business, both financial and otherwise.

2 HOW SHOULD YOU APPROACH DIGITAL TRANSFORMATION?

There is no 'one size fits all' approach to digital transformation. The focus of your digital transformation project should take into account:

- key pain points for your customers in your engagement process;
- key pain points for you in your service delivery process (ie back-end automation);
- areas where your business has unique knowledge or capabilities that can be commoditised; and
- new products, services or data sets you are seeking to develop or leverage.

What are some approaches that can be taken to achieve transformation outcomes?

PROCUREMENT APPROACH: the traditional business process outsourcing approach may allow businesses to achieve efficiencies and cost reductions. However, businesses may need to become comfortable with less legal certainty and the shift away from traditional risk allocation between suppliers and customers.

INVESTMENT STRATEGIES: businesses are increasingly relying on strategic investments in, and partnering arrangements with, third party providers of digital products and services. This approach is a defensive hedge against the disruptive effect of emerging technologies and presents investors with the opportunity to harness and deploy new tech capabilities.

INTERNAL DEVELOPMENT: businesses may choose to build digital solutions internally in order to leverage existing capabilities and retain control or ownership over the digital outputs.

3 HOW WILL YOU STAY ON TOP OF REGULATORY CHANGE?

Regulators are increasingly looking to address digital and data-driven technologies, whether through permissive or restrictive regulatory regimes. In light of this regulatory environment, businesses should:

- consider whether digital transformation projects, and the underlying systems and processes, are able to adapt to incoming regulation; and
- leverage permissive regimes to create value where possible, such as by using the data obtained to more effectively price or provide products to customers, or derive insights and personalise interactions to increase customer loyalty or engagement.

Businesses seeking to leverage data to a greater extent are faced with the challenges of the regulatory landscape regarding the control and use of data, and potential competition issues associated with new commercial models for the use of data.

Digital transformation and the acceleration of focus on digital customer connectivity is upon us and changing how businesses operate and compete. It marks a radical rethinking of how an organisation uses technology, people and processes to fundamentally change business performance.

While there is still a need to comply with regulatory frameworks and internal risk profiles, digital transformation projects provide an ideal opportunity to streamline risk, compliance and operational processes to better position businesses for the future.

WHAT SHOULD YOU DO?

Approaches and regulatory considerations for Digital Transformation.

- When considering digital transformation projects from a legal, risk and compliance perspective, assess which processes are still necessary or fit for purpose and which can be redesigned or altered through the digital transformation project
- Evaluate the pros and cons of different digital transformation approaches to achieve outcomes that are appropriate for your business
- Consider how the regulatory landscape can be leveraged to harness opportunities and achieve digital transformation
- Understand the relevant regulatory frameworks and internal risk profiles to ensure compliance and build resilience against regulatory challenges

Your checklist

A SUMMARY OF THE KEY ITEMS YOU SHOULD CONSIDER IN RELATION TO THE LEGAL ASPECTS OF ACCELERATING YOUR BUSINESS ONLINE.

1. CREATING AND EXPANDING YOUR ONLINE PRESENCE

1.1 Consider your IT infrastructure, your relationships with suppliers and sellers and if your existing IP protections are sufficient

- ☑ When transitioning to the cloud or moving to a new cloud provider, check what is being hosted on the cloud; where the servers are located, including back-up and failover sites; what the scope of the cloud service is; what remains in the business' control or responsibility and what happens when something goes wrong
- ☑ Ensure it is clear who owns the IP rights in your online platform or mobile app
- ☑ Consider if you have adequate licences (if using a standard software product) and the right ownership / licence rights for any customisation
- ☑ Consider patent protection if you develop your own system
- ☑ Ensure you have the appropriate permissions and licences to use and display the content you have on your website, including trade marks and logos
- ☑ Understand your business' position on the use of open source software and on making in-house developed code available as an open source resource

1.2 Remember the sales structure adopted for your online business can have IP, competition and consumer law implications

- ☑ Determine how your online business will be structured from the outset (eg traditional relationship with suppliers as a reseller or as an online marketplace where you may compete with your sellers)
- ☑ Ensure that your pricing and complaints handling policies comply with competition and consumer laws depending on the structure adopted
- ☑ Ensure that you address third party IP infringement risk appropriately depending on the structure adopted

1.3 Consider the security of your payment platform, availability of support and failover measures in place, and how many transactions the platform can handle

- ☑ Ensure that you conduct due diligence prior to selecting your payment platform and have in place robust contractual protections that address liability should the platform fail

1.4 Understand that imposing restrictions on your suppliers or sellers can raise competition law concerns

- ☑ Obtain competition law advice prior to including a 'most favoured nation' clause (or other restriction) in a contract with a supplier/seller
- ☑ Prepare a policy and implement competition law training for employees responsible for the commercial arrangements with suppliers/sellers to ensure they do not discuss or agree impermissible pricing restrictions

1.5 If you offer the products of two competing sellers/suppliers online, be careful what you discuss with each to avoid competition law issues

- ☑ Ensure relevant employees are aware suppliers/sellers may be competitors and provide guidance (eg training, policies) regarding their competition law obligations

1.6 If you sell the products of suppliers/sellers online as well as your business' own products, be aware of the risks of favouring your own products at the expense of the products of other sellers

- ☑ If you are promoting your own business' products above the products of other suppliers/sellers, seek competition and consumer law advice
- ☑ Ensure statements you make about offerings accurately reflect the way your business' algorithm works

1.7 Consider whether you are adequately protected by your existing trade mark registrations for any new or expanded products or services you introduce

- ☑ If you are using a new brand or expanding into new territories or online offering, consider filing new trade mark registrations, as well as domain names and business names

Your checklist

A SUMMARY OF THE KEY ITEMS YOU SHOULD CONSIDER IN RELATION TO THE LEGAL ASPECTS OF ACCELERATING YOUR BUSINESS ONLINE.

- ☑ Undertake a review of your trade mark portfolio to ensure it aligns with your current business priorities and budget
- ☑ If your platform is likely to reach customers in new jurisdictions, consider undertaking clearance / freedom to operate searches to cover these jurisdictions
- ☑ Ensure you have the rights to use any IP sourced from third parties in the digital sphere and in the right jurisdictions
- ☑ Ensure that the content of your website or app does not contain any unlicensed or unauthorised material

2. MANAGING CUSTOMER DATA

2.1 When considering security of data for your business, also consider any specific regulatory obligations

- ☑ Consider practical measures to secure data, such as:
  - appropriate technological access controls (eg, passwords, etc);
  - understanding where data is stored at rest and assessing the suitability of that storage (including location, access controls, back-up procedures, etc);
  - having in place proper retention and destruction policies to ensure only data that must be retained or is actually useful is kept;
  - taking out cyber risk insurance for when, not if, a cyber security incident occurs
- ☑ Put in place a data governance framework to inform your data strategy

2.2 As your business increases its online presence and collects more data, data analytics will become an effective tool to deliver better products and services and an enhanced customer experience

- ☑ Wherever possible, use de-identified data to undertake analytics to minimise the risk of breaching the Privacy Act and embed good privacy practices into every step of the data analytics process

2.3 Understanding the data your business holds offers significant value both to you and other businesses

- ☑ When commercialising customer data, ensure that you understand regulatory limitations, potential restrictions or limitations on the use of that data as well as any other fees that may be applicable

2.4 While increasing your online presence can enhance your business, it is important to understand what privacy laws apply, particularly as some privacy laws have extraterritorial effect

- ☑ Understand what privacy laws apply – if you are reaching a more global market, you may be subject to non-Australian privacy laws
- ☑ Make sure you collect, hold, use and disclose personal information in accordance with any privacy laws that apply, including the Australian Privacy Principles under the Privacy Act
- ☑ Remember that personal information might be valuable data, but you do not 'own' that data and need to use and disclose it, including for analytics, in accordance with applicable law

2.5 Be transparent with customers about how data collected through your online platform or website will be used

- ☑ Be clear with consumers about how their data is being used, particularly if that data is being provided to third parties or for purposes such as advertising
- ☑ Consumers should be given the opportunity to make an informed choice as to whether to explicitly opt out from the collection and use of their data

3. CONNECTING WITH YOUR CUSTOMERS ONLINE

3.1 Understand how you plan to use targeted marketing, particularly as this almost always involves the use of personal information

- ☑ Ensure that any direct marketing complies with the Spam Act and the Privacy Act
- ☑ Be cautious when using personal information to target marketing to individuals, including when targeting ads or offers to customers via Facebook ads or through in-app means (even if that app is your business' app)
- ☑ Understand what data sources your marketing campaigns rely on and how changes to those data sources (such as a move to an opt-in from an opt-out) can impact on your campaigns

Your checklist

A SUMMARY OF THE KEY ITEMS YOU SHOULD CONSIDER IN RELATION TO THE LEGAL ASPECTS OF ACCELERATING YOUR BUSINESS ONLINE.

3.2 Maintain proper records of consent to electronic marketing (eg, via email or SMS) and don't send electronic marketing to anyone who has opted-out

- ☑ Obtain and maintain a list of consents to marketing and maintain a list of opt-outs
- ☑ Wash all marketing campaigns against the opt-out list
- ☑ Make sure that any important factual information (for example, operating changes in response to lockdown measures) is conveyed in a manner that does not blur the line into marketing

3.3 Ensure that savings on products are accurately displayed and do not mislead consumers

- ☑ If making savings representations, ensure it is a genuine saving. This means you have sold the products at the higher price for a reasonable period of time immediately before the promotion price
- ☑ Ensure that you (or your sellers) have sufficient stock for forecast sales during a promotion

3.4 While using sophisticated algorithms which incorporate market data to set prices is useful, price tracking and price setting software may give rise to cartel or concerted practices risks in some circumstances

- ☑ If using AI to set pricing, provide competition law training to those adopting and programming such technology
- ☑ Monitor the effect of any automated decision-making to ensure that it is competition law compliant

3.5 If your online business involves material provided by users (eg a service which prints user-uploaded photos), you may be exposed to liability if the material (or your reproduction of it) infringes copyright or other IP

- ☑ Make sure you have a policy in place that establishes clear standards about the content that your employees and third parties can post on your website or social media pages, and monitor compliance with the policy
- ☑ Implement processes and tools to use to hide or moderate third party comments on your website or social media pages as failing to remove defamatory content once you are made aware of it also exposes you to risk

3.6 If your website displays customer reviews, there is a risk fake reviews can skew ratings and are capable of giving consumers a misleading impression about the product

- ☑ Ensure suppliers/sellers understand what can/cannot be done from a consumer law perspective in relation to customer reviews and incorporate your expectations and requirements into your agreements
- ☑ Monitor reviews to reduce the risk of misleading or defamatory content and IP-infringing material being advertised on your website

3.7 Be aware an increased online presence can lead to an increase in the risk of digital infringement

- ☑ Update your IP monitoring and enforcement strategy to protect against cybersquatting and digital infringement

4. YOUR WORKFORCE ONLINE

4.1 Contingent workforce models that make use of contractor or labour hire arrangements can allow your business to scale to customer demand in the digital environment well, but have risks that need to be managed

- ☑ Consider the relationship you wish to have with your workers or employees and ensure your contracting practices reflect that intention
- ☑ Should your business wish to use labour hire or contractor arrangements, ensure you are aware of the regulatory overlay and any obligations imposed on you (eg in relation to superannuation contributions)

4.2 Regardless of whether your workforce is employee or non-employee based, understand your work health and safety (WHS) obligations in respect of those workers

- ☑ Understand that your WHS obligations extend to digital or remote workplaces and take reasonably practicable steps to ensure that those workplaces are safe. This may include extending WHS practices to cover mental health risks

Your checklist

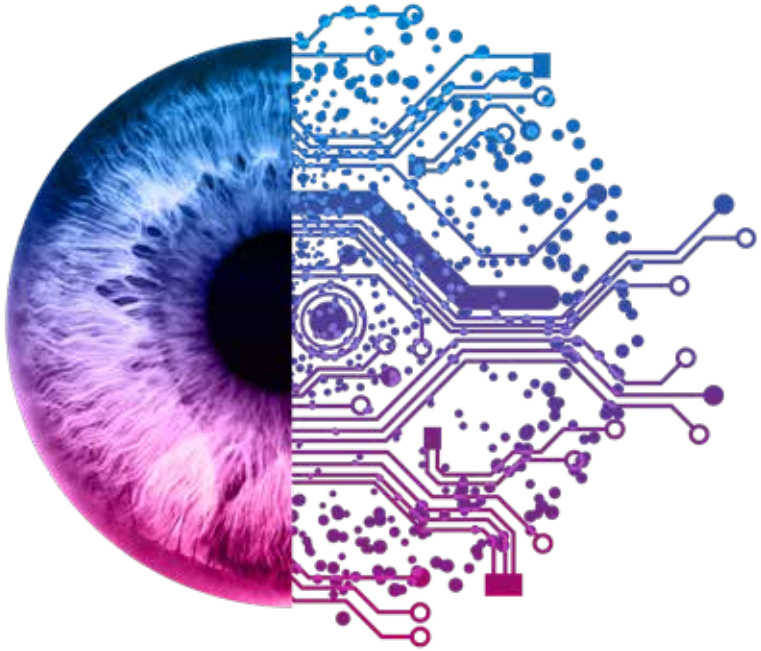
4.3 Forward plan to manage your business' online reputation

- ☑ Ensure employment contracts and zvwvcontractor agreements contain provisions that deal with social media use, disparagement or other conduct that damages the reputation of the business. Consider if agreements provide your business with the right mechanisms to respond to a worker's damaging social media activity
- ☑ Give workers given clear direction about the extent to which (and how) their 'personal' social media presence can be distinguished from online activity as a representative of your business
- ☑ Employ agreements with workers to make clear who 'owns' social media accounts that are used for business purposes

5. DIGITAL TRANSFORMATION

5.1 Ensure you are prepared for digital transformation by putting in place frameworks that enable your business to be agile and flexible when it comes to technology upgrades in the future.

- ☑ Consider areas where you can afford to take some risks (for example, adding a new feature to your app) and where you need to be more cautious (like your critical IT infrastructure).
- ☑ Understand that reliable technology is critical to being a successful business and it pays to invest in current and future technology.
- ☑ Use technology roadmaps as a tool for planning and strategising both the short-term and long-term changes in your business' technology environment.
- ☑ When considering digital transformation projects from a legal, risk and compliance perspective, assess which processes are still necessary or fit for purpose and which can be redesigned or altered through the digital transformation project
- ☑ Evaluate the pros and cons of different digital transformation approaches to achieve outcomes that are appropriate for your business
- ☑ Consider how the regulatory landscape can be leveraged to harness opportunities and achieve digital transformation
- ☑ Understand the relevant regulatory frameworks and internal risk profiles to ensure compliance and build resilience against regulatory challenges



allens.com.au/data-driven-business

Contacts

Rosannah Healy
Partner, Competition, Consumer and Regulatory
T 61 3 9613 8421
Rosannah.Healy@allens.com.au

Veronica Siow
Partner, Employment and Safety
T +61 2 9230 4135
Veronica.Siow@allens.com.au

Gavin Smith
Partner, Technology, Data and Privacy
T +61 2 9230 4891
gavin.smith@allens.com.au

Carolyn Oddie
Partner, Competition, Consumer and Regulatory
T +61 2 9230 4203
Carolyn.Oddie@allens.com.au

Sikeli Ratu
Partner, Employment and Safety
T +61 2 9230 5046
Sikeli.Ratu@allens.com.au

Michael Park
Partner, Technology, Data and Privacy
T +61 3 9613 8331
Michael.Park@allens.com.au

Jacqui Downes
Partner, Competition, Consumer and Regulatory
T +61 2 9230 4850
jacqueline.downes@allens.com.au

Miriam Stiel
Partner, IP
T +61 2 9230 4614
Miriam.Stiel@allens.com.au

allens.com.au

18737D