CyberCX
Privacy by Design

Privacy by Design
Observations in the Australian market 2023

Enhancing privacy management through effective data governance

Privacy by Design **Observations in the Australian Market 2023**

CyberCX's Privacy by Design report is the second edition of CyberCX's analysis over 100 top consumer brands operating in Australia and their performance against the seven globally recognised Privacy by Design principles. In this report, CyberCX uncovers what brands are doing to demonstrate excellence in Privacy by Design.

Contents

Introduction

Since the inception of the seven Privacy by Design principles in the 1990s, we have witnessed events that have been **pivotal to changing the privacy risk landscape** for organisations in Australia and globally. These shifts have ignited a cultural change in the expectations of consumers and citizens for organisations and governments to manage their data appropriately, protect their personal information and uphold their privacy rights.

This includes high-profile data breaches of Australians' personal information by some of Australia's most trusted brands, the increase of enforcement actions by privacy and competition regulators, and the COVID-19 pandemic, which has embedded technology in our lives and spurred innovation in data intensive technologies that leverage individuals' personal information.

In Australia, these and other events have led to proposed changes to privacy law that will see the regime broaden in scope. For example, through expanding the definition of personal and sensitive information and reconsidering exemptions from the law, and introducing enhanced privacy rights for individuals, such as the right to erase their data and limitations on the use of targeted advertising, artificial intelligence and third-party data.

Globally, the International Standards Organisation's adoption of the ISO 31700 on Privacy by Design signals how Privacy by Design is gaining traction worldwide. We have also seen regulators emphasize the value of Privacy by Design, with the Irish Data Protection Commission having imposed a fine of €265 million against a social network for a breach of the principles as they are embodied in the General Data Protection Regulation (GDPR). This indicates to us the global community's growing expectations for their data to be protected against misuse or other privacy invasions.

Noting these events, it is time to reflect on our professional practices and consider the **business and social imperatives** to build not only privacy into the design of our technology, products and processes, but more broadly, data governance to effectively manage the data we hold.

Privacy and data governance approached in the right way can play an important role in **driving better business performance, building consumer trust and attracting new opportunities**. This is needed particularly as organisations' data practices evolve, and privacy and associated data risks increase against a complex regulatory landscape.

The seven Privacy by Design principles, first developed in Canada by former Ontario Privacy Commissioner, Dr. Ann Cavoukian, are built on the idea that privacy and data protection considerations should be built into the design of all organisation systems, processes and products that touch personal information.

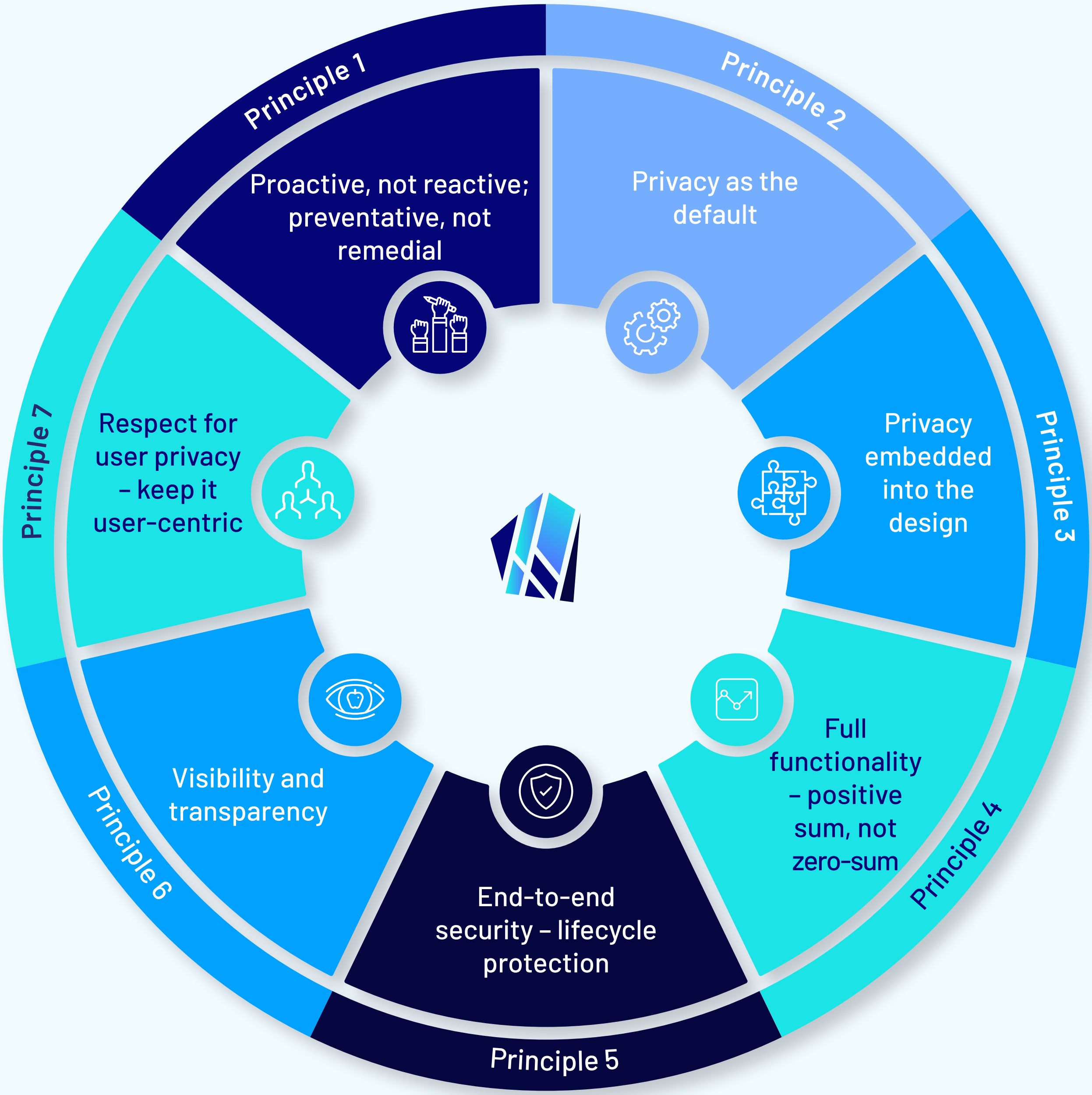
CyberCX's team of researchers have assessed how leading consumer brands operating in Australia across 11 industry sectors have embedded Privacy by Design into their primary web-based customer and user interfaces.

Assessing over 130 unique attributes, each aligned to one of the seven Privacy by Design principles, we've measured the publicly observable features of each brand's web application including privacy attributes, and technical security capabilities that have positive and negative privacy impacts. Using a scoring methodology linked to the risk or benefit each attribute has on an individual, we've been able to determine how each of the industry sectors have performed in embedding Privacy by Design in their digital shopfronts – in particular, in contrast to how the industries performed in 2022.

We present this paper as a snapshot of our insights and findings. We hope our research will ignite meaningful dialogue on privacy and what organisations can do better to realise sustainable and privacy-centric value in personal information and build consumer trust.

Privacy by Design principles

The brand level analysis that has been aggregated to produce the industry level findings in this report has been derived from over 130 different and measurable attributes, each of which maps to one of the seven Privacy by Design principles.


Principle 1
Proactive, not reactive; preventative, not remedial
Principle 2
Privacy as the default
Principle 3
Privacy embedded into the design
Principle 4
Full functionality – positive sum, not zero-sum
Principle 5
End-to-end security – lifecycle protection
Principle 6
Visibility and transparency
Principle 7
Respect for user privacy – keep it user-centric

> *"Privacy by Design is a process for embedding good privacy practices into the design specifications of technologies, business practices and physical infrastructures . This means building privacy into the design specifications and architecture of new systems and processes."*

The Office of the Australian
Information Commissioner

Key insights

CyberCX has captured brands' net performance by sector and how the 11 sectors have performed against each Privacy by Design principle. Overall, CyberCX found that:

- no brand's website successfully implemented the full breadth of measures to achieve Privacy by Design as reflected in the seven Privacy by Design principles
- brands varied considerably in the extent to which they implemented user interface designs, features, or tools for presenting information to accord with the seven Privacy by Design principles
- all brands have significant work ahead of them to successfully realise Privacy by Design in their web shops.

Top performing industries across all seven Privacy by Design principles

#1	Telecommunications & Technology
#2	Food & Grocery
#3	Government
#4	Media
#5	Banking & Finance

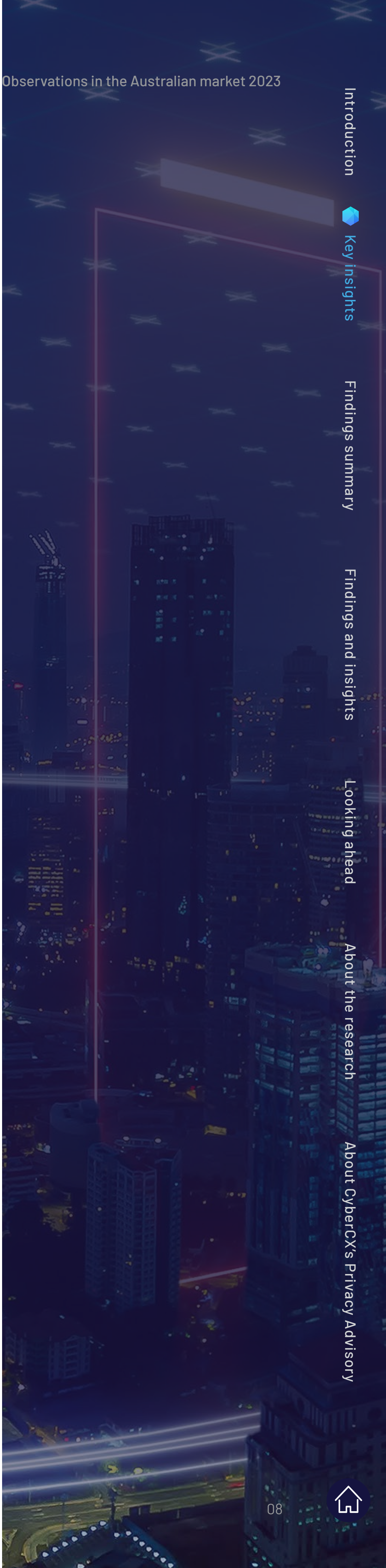
Net Privacy by Design performance by sector

In accordance with CyberCX's methodology, net Privacy by Design performance by sector is reflected by the average of summed normalised Privacy by Design scores for brands within each of the 11 sectors. The maximum possible average score for a sector is out of seven and would be achieved by each of the 9-10 brands within that sector achieving a summed normalised Privacy by Design score of seven. Averaged scores capture the broad trend of the extent to which brands within sectors implement privacy by design for all seven Privacy by Design principles.

CyberCX found that the Telecommunications & Technology sector was the top performer achieving an average Privacy by Design score of 3.11 out of 7 (44.4%) across each of the 10 brands measured within that sector (see Figure 1). That is, the 10 brands within the best performing sector still scored less than 50% for Privacy by Design overall. Average brand performance gradually declined from there with the Health, Fitness & Leisure sector achieving the lowest average score of 1.76 out 7 (25.1%) for the 10 brands measured within that sector. Overall, this result reflects that Privacy by Design is not a strong trend in the design and implementation of digital shop fronts for all 11 sectors assessed. However, as demonstrated via various case studies later in this report, there are stronger, emerging instances of positive Privacy by Design practices being implemented in some web spaces.

Sector performance by principle

This year's Privacy by Design paper highlights that while several sectors performed better than their peers in upholding the seven Privacy by Design principles in their digital interfaces, there are significant opportunities for improvement across the board.



Introduction
Key insights
Findings summary
Findings and insights
Looking ahead
About the research
About CyberCX's Privacy Advisory

Principle 1: Proactive, not reactive; preventative, not remedial

Strong performers turned privacy into a competitive business advantage by taking a privacy by default approach. Some leading brands found in the Banking & Finance sectors developed Privacy Management Policies to establish to staff its expectations on privacy management. Brands found in the Telecommunications & Technology sectors developed and published Privacy Principles that guide them in the design of their products and service offerings.

Principle 2: Privacy as the default

Brands that performed well against this principle employed cookie banners that did not have the most permissive privacy settings by default and provided consumers with the option to easily opt in and out of data practices. Leading brands were found in the Food & Grocery, Telecommunications & Technology and Media sectors.

Principle 3: Privacy embedded into design

Brands that performed well against this principle utilised privacy dashboards that facilitated meaningful control of user's privacy settings. Leading brands were found in the Food & Grocery and Property & Utilities sectors.

Principle 4: Full functionality – positive-sum, not zero-sum

Brands that performed well against this principle balanced seemingly different interests, such as security and privacy. Leading brands were found in the Telecommunication & Technology, Government and Food & Grocery sectors.

Principle 5: End-to-end security - lifecycle protection

Several positive privacy practices were engaged by brands, including a strong encryption in transit granted by the latest Transport Layer Security (TLS) protocols and ciphers, by implementing Multi-Factor Authentication (MFA), and by enforcing the HTTP Strict Transport Security (HSTS). Leading brands were found in the Social Media, Food & Grocery, Telecommunications & Technology and Government sectors.

Principle 6: Visibility and transparency

Brands that performed well communicated their privacy practices in a manner that was open, clear and easy to understand. Leading brands were found in the Government, Media and Food & Grocery sectors.

Principle 7: Respect for user privacy – keep it user-centric

Brands that performed well designed their platforms with the purpose of making it easier for a user to manage their privacy. Leading brands come from the Media, Banking & Finance, Telecommunications & Technology, Food & Grocery sectors.

Net Privacy by Design score - by sector

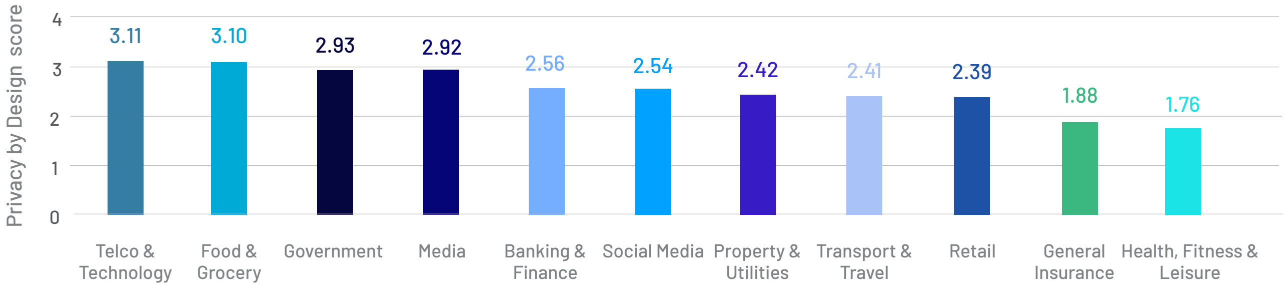


Figure 1: Net Privacy by Design Score - by sector

This plot reflects the average net Privacy by Design score achieved by the sample of brands from each of the 11 sectors. To reflect performance for the implementation of an individual Privacy by Design principle, each brand receives a score between 0 and 1. As such, the net Privacy by Design score is out of 7, given that there are seven principles in total. The average net Privacy by Design score for brands within a given sector reflects the broad trend of the extent to which Privacy by Design has been successfully implemented. Overall, brands across all 11 sectors can take further steps to improve their privacy practices to achieve Privacy by Design.

Sector's performance – by principle

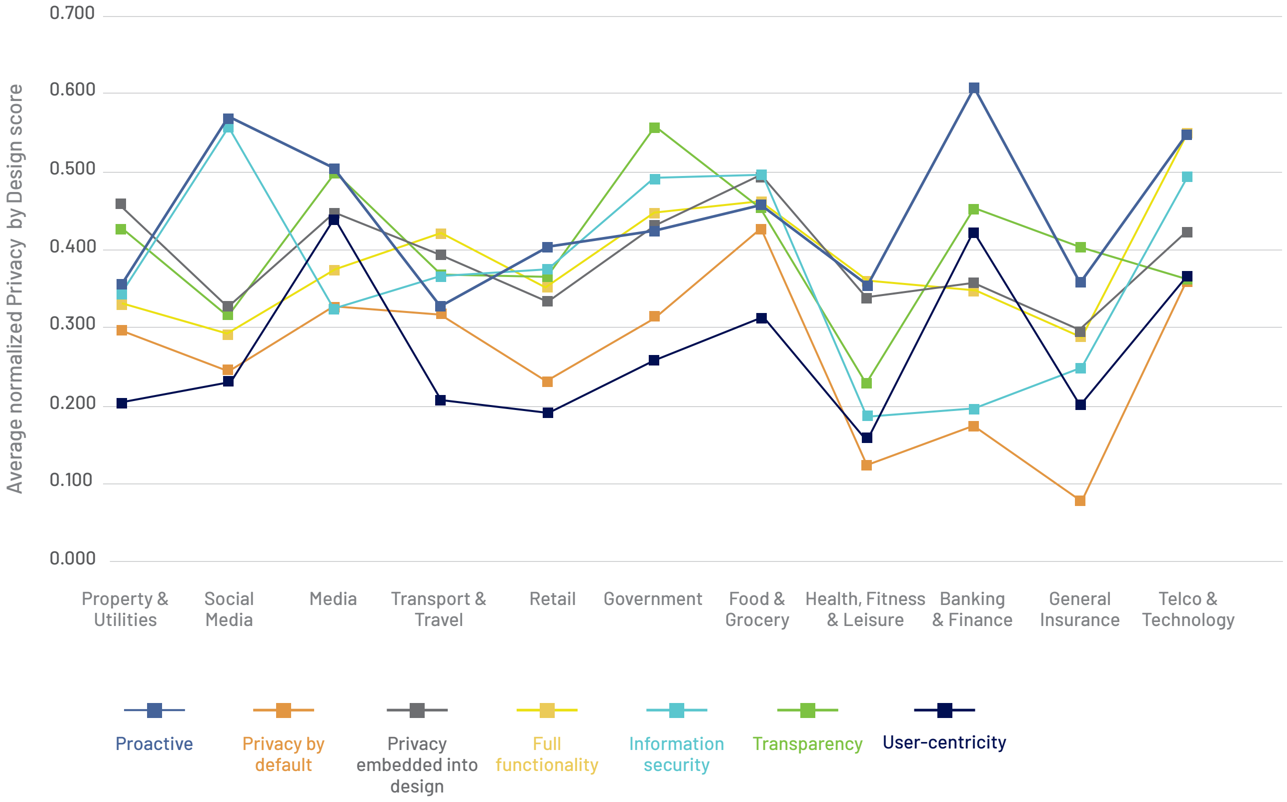


Figure 2: Sector's Performance - by principle

This graph indicates the performance of sectors against each of the seven Privacy by Design principles. While some sectors performed well against some principles, they perform poorly against other principles, indicating areas of improvement across the 11 sectors.

> *“Privacy by Design advances the view that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organisation’s default mode of operation.”*

Dr Ann Cavoukian
Former Information and Privacy
Commissioner, Ontario, Canada

Findings summary

In an age where data breaches abound and privacy invasions continue to proliferate, taking a Privacy by Design approach is crucial for organisations to reduce their privacy risk, build consumer trust and confidence in their handling of personal information, and go beyond minimum compliance with legal obligations to model privacy best practice.

By applying the seven foundational principles into the design of your applications, systems, products and business processes and embedding strong data governance within your organisation, privacy can become a meaningful point of differentiation for organisations that want to achieve a competitive business advantage, while helping to ensure that individuals' have meaningful control over their personal information.

Findings

In our analysis of which brands uphold Privacy by Design in the most meaningful ways, we focused on positive privacy practices brands were engaging in the areas of openness and user transparency, user consent and notification, user-centricity, and information security. To assess for the negative privacy impacts of certain practices, we examined how brands were using tracking technologies to identify and track users online, as well as dark patterns as part of a user's web experience to 'nudge' or manipulate users toward behaviours that would reduce their privacy online.

Overall best performers

Similarly to last year's results, the Telecommunications & Technology sector performed the strongest overall across all seven Privacy by Design principles. This was achieved through undertaking several positive privacy practices, including by providing individuals with greater access and control over their privacy settings, developing privacy or security dashboards, publishing educative material on privacy and security, and minimising the use of negative practices which result in 'reactive' approaches to privacy management.

Good practices observed

The brands that differentiated themselves from the rest and performed better:

- designed capabilities to enable consumers to manage their personal information, enforce their privacy rights and determine their privacy preferences
- took proactive steps to educate readers about how they could meaningfully control their privacy settings, and
- took a privacy by default approach to their communications and design of their digital interfaces.

Areas for improvement

The brands that performed the worst:

- had room for improvement in the transparency and clarity of their communication on their privacy practices. Some brands Privacy Policies did not fully meet legislative requirements, performed poorly on readability tests, and were less accessible to users. Other brands had poor notice and consent practices, with some brands not having Privacy Collection Notices in place at a point of collection
- embedded more privacy invasive tracking technologies as part of a user's web browsing experience than the average brand, and
- engaged in more third-party data sharing, including with advertising companies.

Key takeaways

Australia's anticipated privacy law reform will likely materially change the way Australian organisations approach privacy compliance.

CyberCX's research indicates that there will be an increasing imperative for organisations to get "back to basics," the theme of this year's Privacy Awareness Week and uplift its foundational privacy practices in order to meet the enhanced standards for privacy management.

Findings and insights

Principle 1

Proactive, not reactive; preventative, not remedial

What is this principle about?

Organisations must be privacy-centric and take a proactive approach that anticipates and manages privacy risks before they occur, rather than a reactive, ad-hoc approach to responding to privacy intrusive events. Privacy by Design comes before-the-fact, not after.

Findings

Sector ranking	
#1	Banking & Finance
#2	Social Media
#3	Telecommunications & Technology
#4	Media
#5	Food & Grocery
#6	Government
#7	Retail
#8	Property & Utilities
#9	Health, Fitness & Leisure
#10	General Insurance
#11	Transport & Travel

In practice

✓ **Commitment to privacy**
Demonstrate a clear commitment to establish and enforce high standards of privacy

✓ **Privacy strategy**
Data privacy is a strategic priority and brands have a well-defined Data and Privacy Strategy

✓ **Privacy awareness & education**
Users and staff are educated about their organisation's data practices and maintain transparency

Case studies

Privacy centre

Some brands have taken a proactive approach to privacy by establish a privacy centre where users can access a repository of helpful information related to privacy. These privacy centres contain information about:

- explanations on the brand's privacy practices and data policies
- explanations on how users could navigate the platform to manage their privacy, and
- short videos or blogposts on privacy and privacy management.

As a result, users are educated about data practices and transparency is maintained.

Privacy principles

One brand published privacy principles externally, having modelled these after the Fair Information Practice Principles. The brand developed these principles to help its team do more than what is legally required with users' data in the design of its products and services. Some of the principles included:

- doing the right thing with data
- building privacy into the design of products from start to finish
- the need to apply the data minimisation principle
- being transparent about data practices
- providing users with choices about their data, and safeguarding personal data.

Privacy was also reported as part of the brand's environmental, social and governance annual reporting.

Average sector score – proactive principle

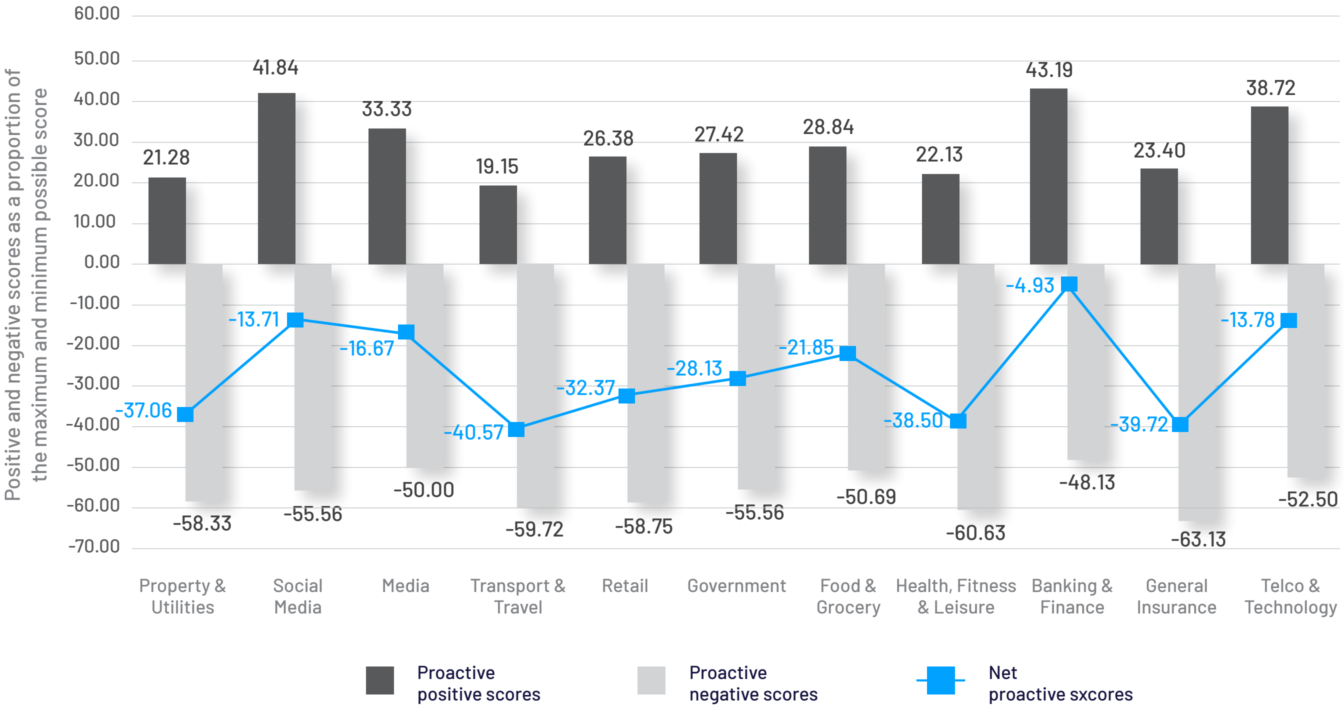


Figure 3: Average sector score – proactive principle
Brands' positive scores against this principle are listed in dark grey bars which reflect the average proportion (percentage) of the maximum possible positive score achieved by each sector against this principle. Negative scores are listed in light grey bars which reflect the average proportion (percentage) of the maximum possible negative score achieved by each sector. The Net Proactive Score (blue line) is the sum of the positive and negative scores. This line reflects the overall performance of each sector on average against the set of metrics used to measure performance against this principle.

Results

Overall, brands across all 11 sectors undertook more negative privacy practices when balanced out with the positive privacy practices. In some sectors, such as the Transport & Travel sectors and Health, Fitness & Leisure sectors, this led to significantly negative net scores against this principle. The negative privacy practices engaged by brands include not taking proactive steps to inform individuals of their privacy and data practices.

Overall best performers

The Banking & Finance sectors reflected the strongest overall embodiment of this principle out of the 11 sectors tested. This result was achieved in part via clear public statements attesting to broad commitments to user privacy with clear information regarding positive privacy practices.

Worst performers

The Transport & Travel and the General Insurance sectors produced the lowest average negative scores against this principle. Negative scores were given to brands within this sector given a consistent trend in publishing privacy policies which do not:

- meet requirements under Australian Privacy Principles (APPs) 1.3 and 1.4, or
- those recommended by the Office of the Australian Information Commissioner in published guidance, such as chapter one of the Australian Privacy Principles Guidelines.

Areas for improvement

Similarly to last year's results, brands could undertake several measures to take a proactive approach to privacy, including by taking steps to inform customers in a transparent and open manner of their privacy practices and initiatives that have undertaken to raise the bar for privacy.

Principle 2

Privacy as the default setting

What is this principle about?

Privacy by Default practices ensure that users don't have to worry about their privacy settings when engaging online as the maximum degree of privacy protections are built into settings. No action is required on the part of the individual to protect their privacy – it is built into the system, by default.

Findings

Sector ranking	
#1	Food & Grocery
#2	Telecommunications & Technology
#3	Media
#4	Transport & Travel
#5	Government
#6	Property & Utilities
#7	Social Media
#8	Retail
#9	Banking & Finance
#10	Health, Fitness & Leisure
#11	General Insurance

In practice

✓ **Data minimisation**
Only the data that is necessary is collected. Don't collect data for the sake of collection or because you can

✓ **Marketing and tracking**
Marketing and tracking technologies are switched off by default. Customers and users must opt-in to such collection

✓ **Security**
Appropriate technical security measures are implemented, such as encryption to ensure the confidentiality, integrity and availability of personal information

Case studies

Opt-out by default cookie model

While CyberCX found that most cookie banners did not facilitate comprehensive or meaningful control over a user's cookie preferences with many adopting an opt-out by default model, one brand demonstrated this principle by developing a Cookie Preference Centre that opted users out of the collection of several cookies by default. This includes:

- targeting cookies: targeting cookies collect user's information and use these to show personalised advertisements to that specific user
- functional cookies: functional cookies help enhance the functionality and performance of a website
- performance cookies: performance cookies or also known as Google Analytics cookies, collect data on the behaviour of a visitor on a website, including page visits, idle time by a user on a page, load speeds and bounce rates.

By opting users out by default of the collection of their personal information, brands can provide users with meaningful choice and control on whether to accept or reject a collection and respect their privacy choices.

Average sector score – privacy by default principle

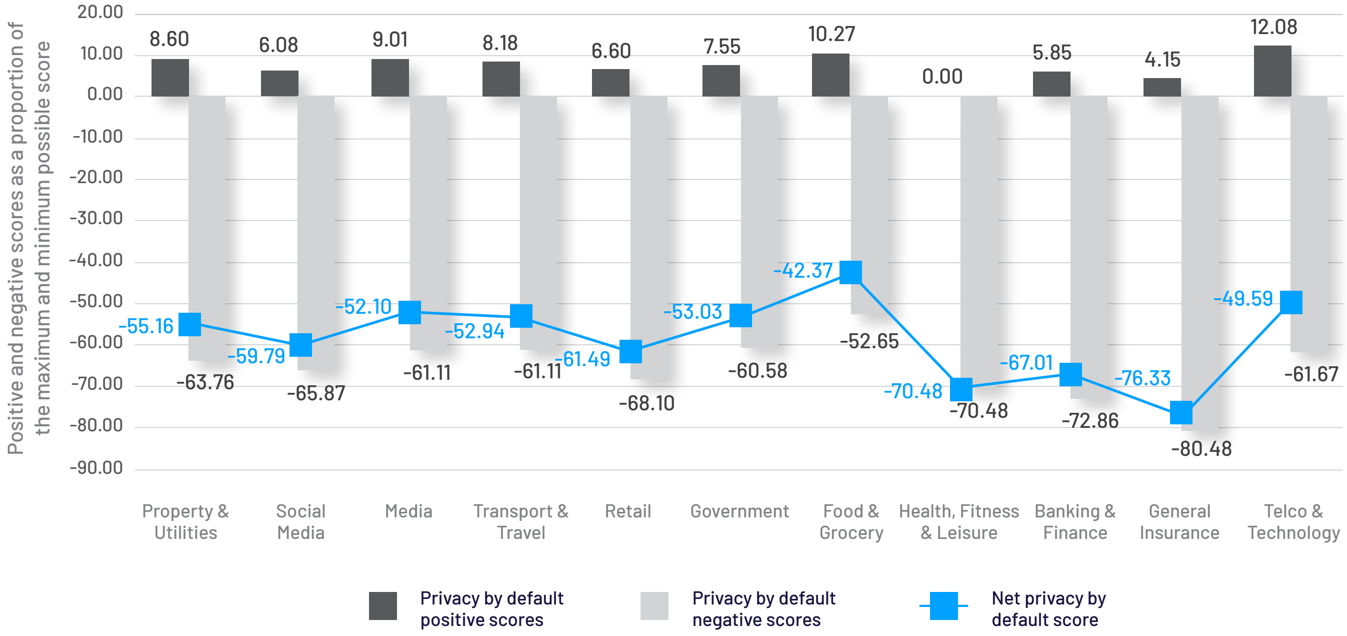


Figure 4: Average sector score – privacy by default principle

Results

Overall, brands across all 11 sectors undertook more negative privacy practices when balanced out with the positive privacy practices. This led to a significant decrease in brands' overall net scores against this principle. The negative privacy practices engaged by brands include the use of dark patterns to encourage users to opt into the unnecessary collection and use of their personal information, and having the most restrictive cookie and analytics settings on their web fronts by default.

Overall best performers

The Food & Grocery sector produced the strongest overall Privacy by Default principle out of the 11 sectors tested at 12%. Despite this positive result, the overall poor performance demonstrates that privacy is not implemented by default in accordance with CyberCX metrics.

Worst performers

The General Insurance sector produced the lowest score by affecting practices which required the collection of personal information from individuals where there were few controls in place to opt out of collection.

Areas for improvement

The lower scores show that there are opportunities for brands across the 11 sectors to implement stronger controls and defaults for privacy to be protected by default, such as using opt-out models for the collection of personal information.

Understanding tracking technologies

As part of this study, CyberCX used The Markup's Blacklight Real-Time Website Privacy Inspector tool to understand who could be identifying, tracking or profiling you as you browse the web, work, shop or learn. Our results demonstrate the prevalence of online tracking across web applications and opportunities for improvement for brands who want to implement Privacy by Design.

How are brands using tracking technologies?

CyberCX found that brands used a wide range of tracking technologies to track visitors, from capturing how users move their mouse, to using trackers to send user data to third-party companies. This leads to intrusive privacy practices that may not be known to users, and if known, are contrary to their expectations.

Advertising trackers

CyberCX found that

95 out of 104

brands deployed ad trackers from three or more ad tech companies

Ad tracking technologies loads JavaScript codes or invisible images that can be used to identify and profile users for ad targeting purposes. The greater the number of ad tech companies involved in tracking users, the greater the potential distribution of user profiles across the internet to a greater number of entities for marketing and advertisement purposes.

Third-party cookies

CyberCX found that

72 out of 104

brands deployed ad trackers from three or more ad tech companies

Websites use cookies to remember a user's preferences for optimal user experience. Third-party cookies are placed by websites other than the website the user is visiting through adding scripts or tags. They are usually used for online-advertising purposes.

Canvas finger printing

CyberCX found that

93 out of 104

brands used canvas finger printing

Browsers generate a lot of information which can be used to create a unique profile of users called fingerprint. Fingerprints can be used to uniquely identify individuals with a high degree of accuracy. Canvas fingerprinting is a type of "browser fingerprinting" technique used to track online users, even if they block third-party cookies.

Facebook pixels

CyberCX found that

92 out of 104

brands used Facebook pixels

The Facebook pixel is a code that sends data back to Facebook about users who visit a website and allows the website operator to later target them with ads on Facebook.

Session recording services

CyberCX found that

96 out of 104

brands used session recording software

Session recorders track user's clicks, mouse movements, scroll and even network activity. Websites that use session recorders compile this information into heat maps and videos so that the owners of the website can watch to see how users interact with the site. According to the Mark-up, research has shown that these practices are insecure and create sensitive user data.

Google Analytics

CyberCX found that

94 out of 104

brands used Google Analytics

Google Analytics is a web analytics service offered by Google that allows brands to track and report on website traffic. This feature allows a website to build custom audiences, based on how a user interacts with a particular website, and then follows those users across the internet and targets them with advertising on other sites using Google Ads.

Source: The Mark-Up Blacklight, https://themarkup.org/blacklight.

Principle 3

Privacy embedded into design

What is this principle about?

When designing the architecture of systems, websites, mobile applications or software, privacy should be embedded into all design aspects – not bolted on at the end, after the fact.

Findings

Sector ranking	
#1	Food & Grocery
#2	Property & Utilities
#3	Media
#4	Government
#5	Telecommunications & Technology
#6	Transport & Travel
#7	Banking & Finance
#8	Health, Fitness & Leisure
#9	Retail
#10	Social Media
#11	General Insurance

In practice

✓ **Embed Privacy by Design**
Privacy by Design is implemented into web and mobile applications, technologies, and systems to the greatest extent possible, without impairing their functionality

✓ **Use, retention & disclosure limitation**
Data is not collected for any other purpose than which the user has agreed to. Data is not kept for longer than is needed

✓ **Cookie banner**
When using cookie banners, ensure users hare allowed to opt in/out

Case studies

Cookie banners

CyberCX found that only 9 of 104 surveyed brands presented a cookie banner to users when accessing their websites. While presentation of a cookie banner does not necessarily represent a positive step toward implementing the principle of embedding Privacy by Design, the layout and ease of use of a cookie banner can have significant impacts on user privacy. For example, cookie banners can be designed to force users to opt-in to accept all cookies by default, therefore, precluding users with possessing meaningful choice. Therefore, an important lesson is for brands to design cookie banners in a way that upholds user-privacy.

Average sector score – privacy embedded into the design

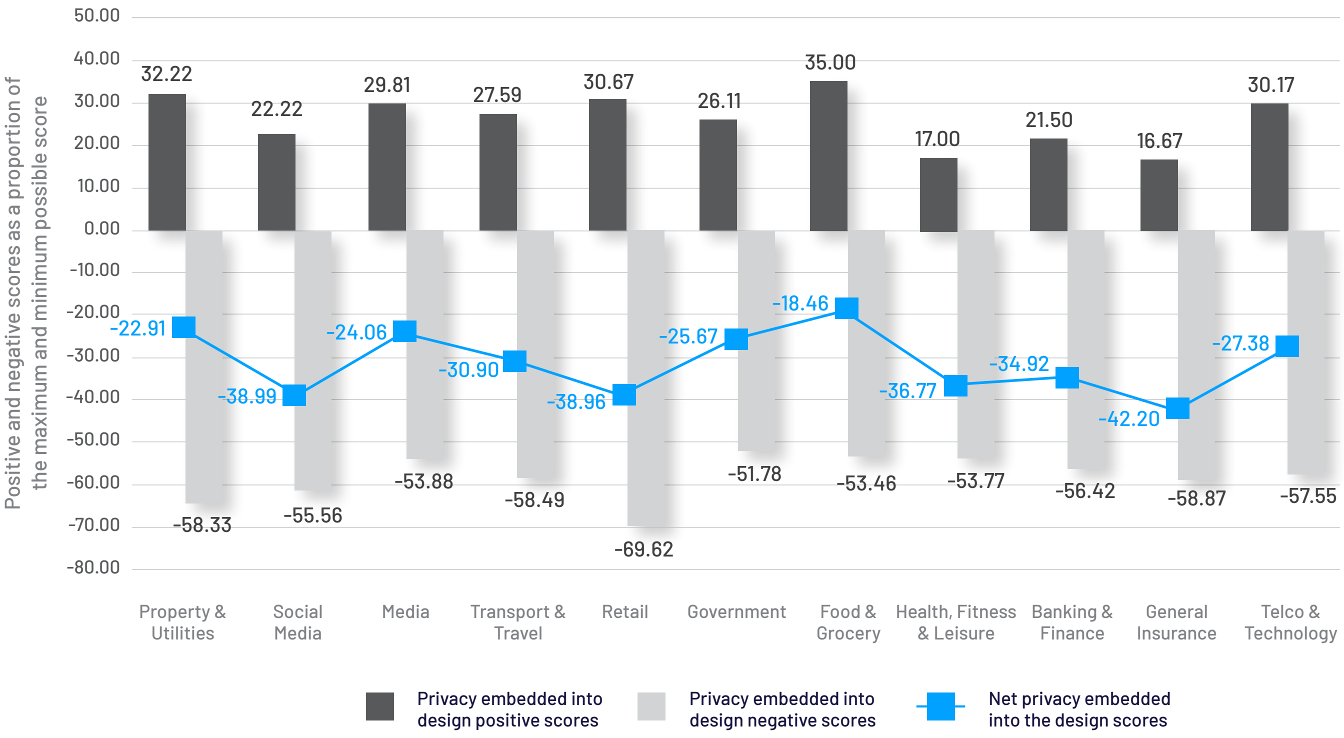


***Figure 5:** Average sector score – privacy embedded into the design*

Results

Brands across all 11 sectors undertook more negative privacy practices when balanced out with the positive privacy practices. The negative privacy practices engaged by brands include not providing consumers with privacy consent notices when collecting personal information from sources such as cookies, not including privacy collection notices at critical collection points, and displaying a lack of transparency in the design of existing privacy notices. Furthermore, 72% of all brands deployed third-parties cookies owned and operated by three or more brands. The greater the number of entities with third-party cookies operating on a given web platform, the greater the distribution of user data across the internet.

Overall best performers

There was mixed, but generally poor performance across the 11 sectors for the privacy embedded into the design principle with Food & Grocery being the top performer with the top score of -35%. For example, Food & Grocery brands generally did not require individuals to register their personal details to use a site for superficial uses or casual encounters.

Worst performers

There was relatively consistent performance across the 11 sectors with there being only a 16.3% differential between the top and worst performers. General Insurance sector brands produced the lowest net score overall in part due to the deploying several ad trackers owned by distinct entities across their web platforms. In other words, retail sector brands typically embed ad trackers into their web shops by design.

Areas for improvement

In general, brands can undertake a range of practices to improve their performance against this principle, including by obtaining meaningful consent for the use of cookies and tracking technologies, and reducing their online profiling, tracking and monitoring of user's activities on web platforms.

Principle 4

Full functionality: positive sum, not zero-sum

What is this principle about?

Organisations that take a positive-sum, "win-win" approach integrate privacy with other legitimate objectives and interests, such as security or user experience – this avoids trade-offs or limitations on functionality from occurring should users want to share less personal information.

Findings

Sector ranking	
#1	Telecommunications & Technology
#2	Government
#3	Food & Grocery
#4	Transport & Travel
#5	Health, Fitness & Leisure
#6	Banking & Finance
#7	Media
#8	Property & Utilities
#9	General Insurance
#10	Retail
#11	Social Media

In practice

✓ **Enable full functionality**
Brands use solutions that enable multi-functionality so that legitimate interests and objectives can be achieved

Case studies

One example of the antithesis of Full Functionality is where brands require users to register their personal information to access site features or services for features or services that do not obviously need personal information to work. True Full Functionality, in this case, is where users are unencumbered by a requirement to provide their personal information to access otherwise free website features or services that shouldn't otherwise require the provision of personal information.

Many users will be familiar with the experience of wanting to read a report on a website, only to find they have to provide your email and other personal details for marketing purposes to access the report. CyberCX found that 90% websites surveyed do not engage in practices where the price of full functionality is the provision of a user's personal information. This represents a positive step in the right direction for full functionality.

Average sector score - full functionality[1]

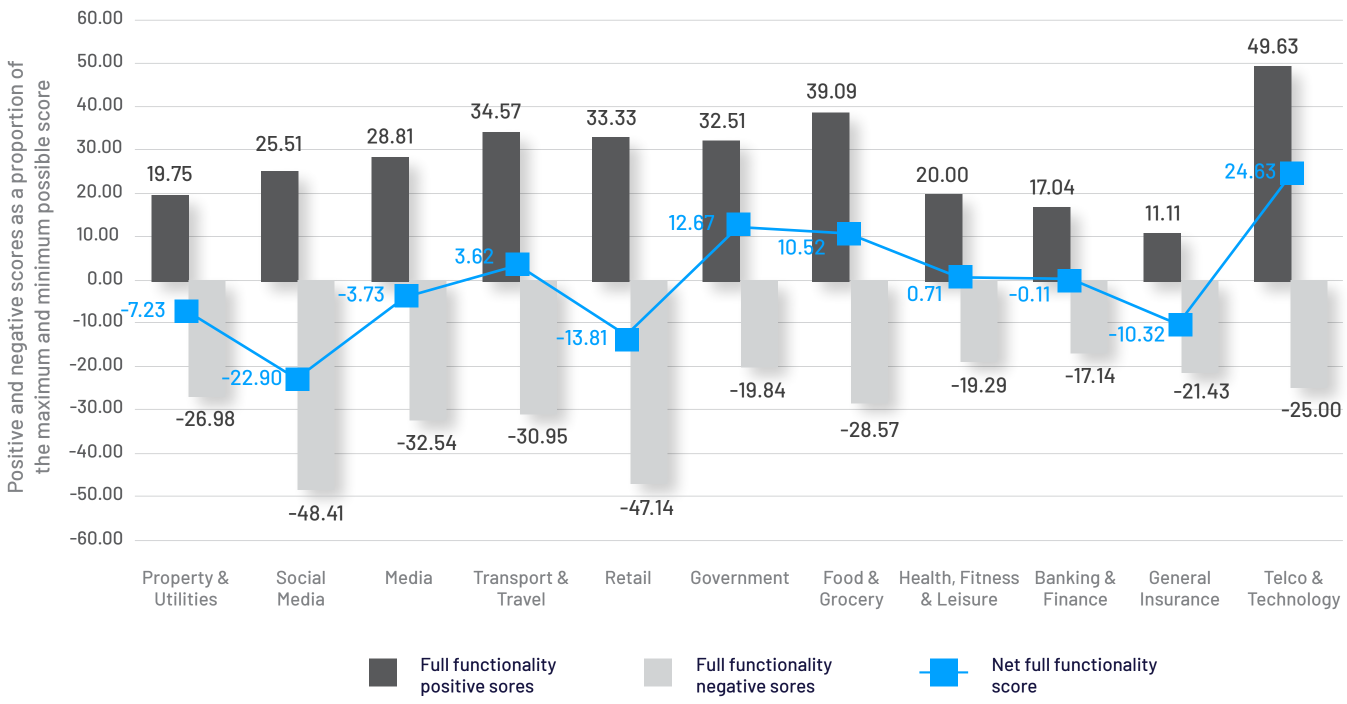


Figure 6: Average sector score - full functionality[1]

Results

CyberCX observed a range of positive and negative practices across the 11 sectors with some sectors engaging in more negative privacy practices, such as the Social Media and Retail sectors, and one sector leading the way in its positive privacy practices (Telecommunications & Technology). This produced a notable variance in the net score against this principle, with 24.6% being the highest score achieved (Telecommunications & Technology) and -22.9% being the lowest score (Social Media). A positive practice CyberCX observed was that the majority of brands (92/104) do not engage in the practice of requiring individuals to provide their personal information (e.g., via a registration process) to use the basic features of the website.

Overall best performers

The Telecommunications & Technology sector was the best performer for the Full Functionality principle. For example, 8 out of 10 Telecommunications & Technology brands provide users some capacity to download information about themselves without having to lodge formal requests with the brand's privacy officer.

Worst performers

Overall, most brands from all 11 sectors did not provide users with full functionality by bundling consents for cookies and ad-tracking technologies, thereby removing user control to opt-in to or out of cookies and tracking.

Areas for improvement

An area where many brands could boost website 'full functionality' is by giving users full control over the array of cookies and tracking features in such a fashion that does not come at the cost of the accessibility to services or of the functionality of the website and its various features.

Principle 5

End-to-end security – full lifecycle protection

What is this principle about?

Organisations can protect users' personal information by implementing end-to-end security throughout the personal information lifecycle. This includes from when data is collected, to when it has served its purpose and can be destroyed.

Findings

Sector ranking	
#1	Social Media
#2	Food & Grocery
#3	Telecommunications & Technology
#4	Government
#5	Retail
#6	Transport & Travel
#7	Property & Utilities
#8	Media
#9	General Insurance
#10	Banking & Finance
#11	Health, Fitness & Leisure

In practice

✓ **Security**
Appropriate technical security measures are implemented, such as encryption to ensure the confidentiality, integrity and availability of personal information

✓ **Data Retention**
Data retention periods for users' data are defined; indefinite retention is never acceptable

Case studies

Raising awareness of scams

Several brands assessed from the Food & Grocery and Banking & Finance sectors published dedicated pages in their website with educative information about scams as well as helpful tips about identity protection and online security. Scams generally cause financial loss to victims; therefore, the more well-prepared users are in identifying scams, the sooner they will be able to take action to avoid losses and harms from occurring.

Promoting cybersecurity knowledge

The theme of this year's Privacy Awareness Week is *Back to Basics*, and one brand from the Telecommunication & Technology sector demonstrated a commitment to raising awareness of the role individuals play in the protection of their information online. The brand offers free security basics training that includes quizzes to assess the knowledge users gained and provides users with a Security Champion badge upon successful completion.

Average sector score – information security

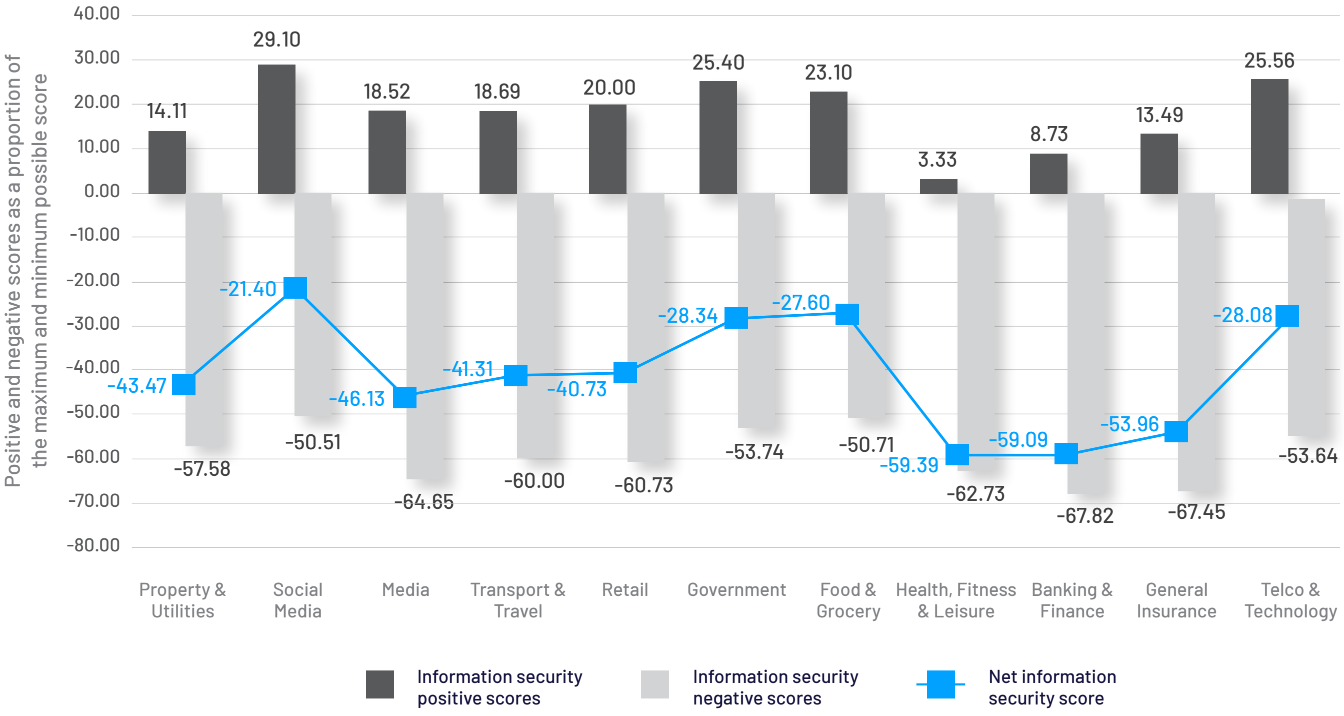


Figure 7: Average sector score – information security

Results

Brands across all sectors did not perform well against this principle, with all brands scoring at least -50% for negative privacy practices, which consequently reduced brands' performance on the net score for the End-to-end Security principle. The high rate of negative scores were due to the widespread use of ad-trackers, key loggers, the disclosure of information to ad-tech companies, and allowing the operation of persistent third-party cookies across almost all brands assessed. This indicates that there is much improvement to be had information security across the board.

An emerging trend is the provision of a website feature which grants users the ability to request that brands delete the data they hold about them. This functionality is a distinct practice from account deletion which may or may not be used to yield a similar effect. CyberCX found that at this stage, 18.2% of brands measured provide this feature. Should the Australian law reform process result in a legislated right to erasure, more brands will need to provide personal information erasure services to users.

Overall best performers

Overall, the Social Media sector led in performance against this principle with the Telecommunication & Technology, Government, Food & Grocery sectors closely behind. Positive scores were due to affecting positive practices such as providing users the option to further secure their accounts with multi-factor authentication. 40% of brands from the Social Media sector provide users the option to delete some or all of the data the brand holds about that individual.

Worst performers

The Banking & Finance and General Insurance sectors underperformed compared to other sectors, due to the widespread use of keyloggers and practices such as not enforcing HSTS[2] and CSPs[3].

Areas for improvement

Brands could focus on removing the use of user-tracking technologies that pose information security and privacy risks, such as key loggers as well as ensure the currency of Transport Layer Security (TLS)[4] protocol configuration across their web platforms. For example, CyberCX found that 50% of brands deploy persistent third-party cookies on their websites.

Principle 6

Visibility and transparency – keep it open

What is this principle about?

To build accountability and trust, organisations should be open and transparent about their privacy policies and data practices, letting users know upfront about their what they're doing.

Findings

Sector ranking	
#1	Government
#2	Media
#3	Food & Grocery
#4	Banking & Finance
#5	Property & Utilities
#6	General Insurance
#7	Transport & Travel
#8	Retail
#9	Telecommunications & Technology
#10	Social Media
#11	Health, Fitness & Leisure

In practice

✓ **Openness and transparency**
Brands provide information about its data practices, and privacy policies and procedures are openly available to individuals

Case studies

Transparency drives trust

One brand from the Telecommunication & Technology sector published Privacy Nutrition Labels to help users understand how applications handle their data. The kind of information shared to the user includes:

- what kind of data may be collected and linked to users' identity by the organisation
- the kind of data not linked to a users' identity by the organisation.

A link to the organisation's privacy policy is provided. This initiative is intended to promote transparency and user awareness of organisation's privacy practices, particularly in an age where organisations' data practices are often opaque.

Taking a strategic approach to privacy management

A privacy management plan is a document that enables an organisation or agency to strategically plan for how they will reach their privacy management goals and objectives. One state government agency brand published its Privacy Management Plan (PMP) on their website. The document has several pages and provides practical guidance to staff on how to manage personal information, in line with the values and expectations of the agency.

Average sector score – user transparency

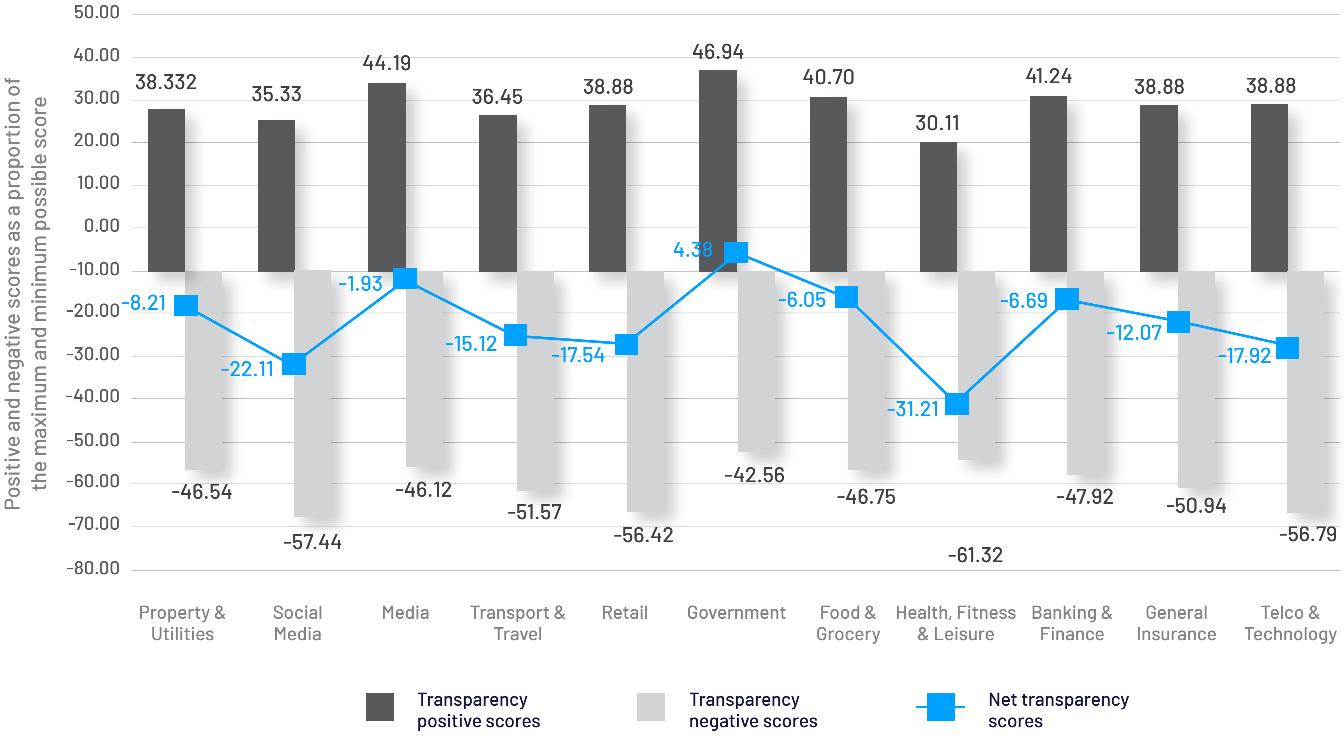


Figure 8: Average sector score –user transparency

Results

Brands across all 11 sectors engaged in more negative privacy practices, in contrast with the positive privacy practices they engaged in. For example, the Social Media sector has the lowest score of -57.44% due to the prevalence of negative privacy practices, with the Telecommunications & Technology sector not far behind with the second score of -56.79%. The negative scores across all 11 sectors led to overall low net scores against this principle.

Overall best performers

The Government sector was the top performer overall. Positive performances were due in part to clear, easy to read, comprehensive, layered, and accessible Privacy Policies and Privacy Collection Notices.

Worst performers

The Health, Fitness & Leisure, Retail, Social Media and Telecommunications & Technology sectors produced lower in scores on average, due to factors such failing to present comprehensive, clear privacy notices that accord with all of the requirements of Australian Privacy Principle 5. These practices are likely to impact the degree to which users are made aware of brands' practices regarding their data collection and use.

Areas for improvement

Consistent with brand's performance last year, an area for improvement for most sectors relates to the readability of Privacy Policies and improvements in their Privacy Collection Notices. To improve their performance, brands should ensure that they clearly communicate their personal information handling practices using language that is free of jargon and easy to understand and take steps to enhance the accessibility of their Privacy Policy. For example, through layering their Privacy Policies or providing supplementary mediums by which users can understand the brand's privacy practices, such as leveraging video to communicate its privacy practices.

Principle 7

Respect for user privacy: keep it user centric

What is this principle about?

To ensure user-centred privacy, organisations can implement safeguards and features that make privacy management easy. This includes by using strong privacy defaults, meaningful notices, and user-friendly options and controls.

Findings

Sector ranking	
#1	Media
#2	Banking & Finance
#3	Telecommunications & Technology
#4	Food & Grocery
#5	Government
#6	Property & Utilities
#7	Social Media
#8	Transport & Travel
#9	General Insurance
#10	Retail
#11	Health, Fitness & Leisure

In practice

✓ **User-friendly controls**
Provide users with meaningful choice and control about how their personal information is handled

✓ **Meaningful user choice**
Brands avoid pre-ticking checkboxes which steal away the choice a user may exercise

Case studies

Several brands developed privacy dashboards accessible in consumer's authenticated environments as a tool to manage their privacy settings for the services and products they use, and a tool to help facilitate meaningful access and control over their personal information. Some brands demonstrated privacy best practice by providing users with the option to access the data held about them and delete it and begin removing it from brands' systems. Other kinds of personal information, such as service data and app information may be shared by the brands' third-party providers when individuals log into their accounts. Some brands provided the consumer with the ability to disable this third-party data sharing, which is a pleasing practice to see.

Average sector score – user centricity

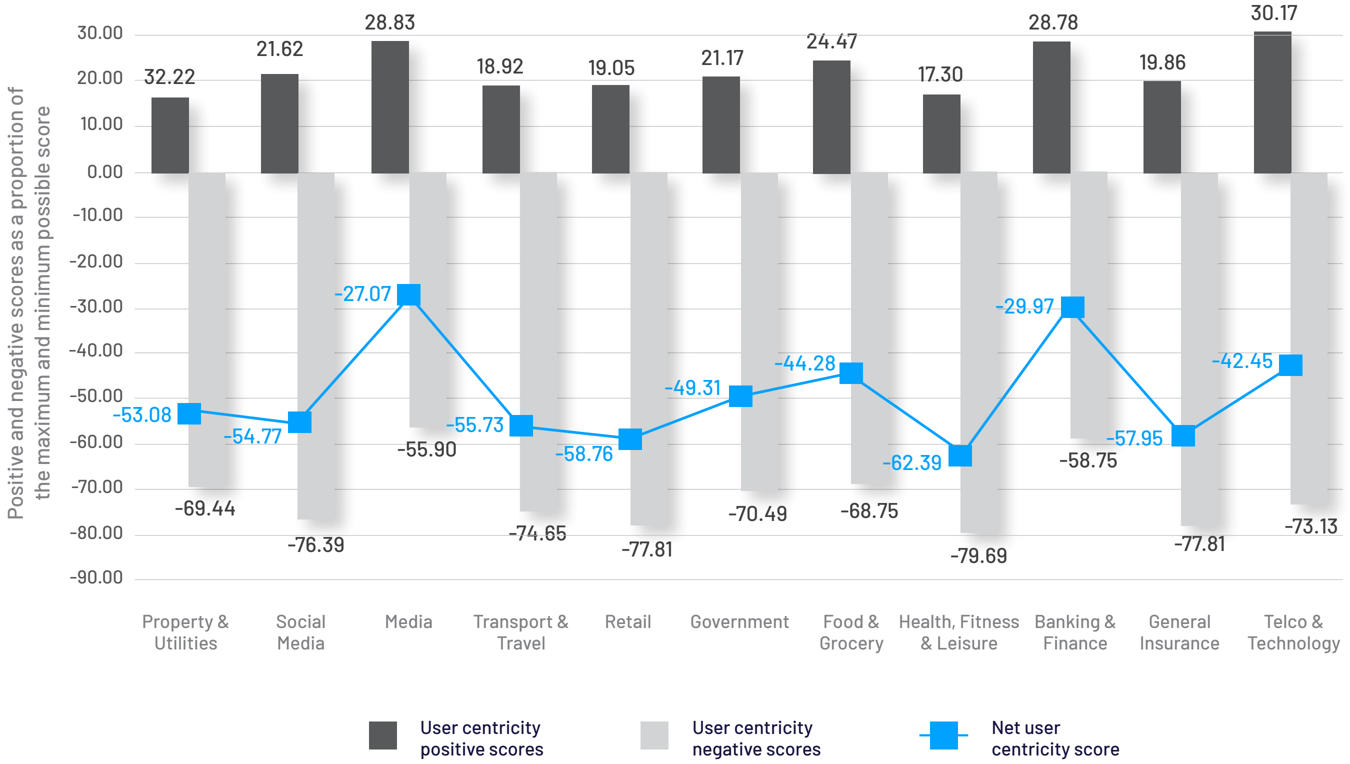


Figure 9: *Average sector score – user centricity*

Results

All sectors performed poorly against this principle with the average negative score against this principle being -71.16%. This demonstrates that there are significant areas of improvement across the board toward ensuring user-centred privacy in the design of web applications and features for privacy management. Most Australian based websites did not provide users with graphical interfaces that made it easy for individuals to control what cookies, tracking technologies and analytics technologies operated on their web platforms.

Overall best performers

The Media sector produced the highest overall average score for this principle. The sector's higher positive scores relative to the other sectors demonstrate a public commitment to privacy via the publication of blog posts or other media on privacy and cyber security issues. These practices demonstrate a public commitment to respecting user-privacy.

Worst performers

All 11 sectors surveyed produced consistently low average scores overall due to challenges such as the failure to present clear and easy to locate privacy notices describing the brands personal information management practices at the point of the collection of personal information. In most cases, brands did not present a privacy notice that fulfill the requirements of APP 5. Rather, brands presented generally single sentence statements regarding agreement to a hyperlinked privacy policy when collecting personal information.

Areas for improvement

For brands to improve their performance against this principle, they should provide users with controls regarding the operation of cookies, tracking technologies and analytics technologies on their digital interfaces. When designing these controls, brands should avoid the use of dark patterns which encourage users to opt-in to features that may not be in the best interest of their privacy such as by making the 'accept all' button the most prominent button.

Looking ahead

After a long-running review of Australia's privacy laws, the Attorney-General's Privacy Act Review Report has released 116 recommendations that, if adopted, will see significant changes to the future of privacy in Australia.

The recommended reforms will have major implications for business and government, as well as individuals that will see the introduction of new privacy requirements, such as:

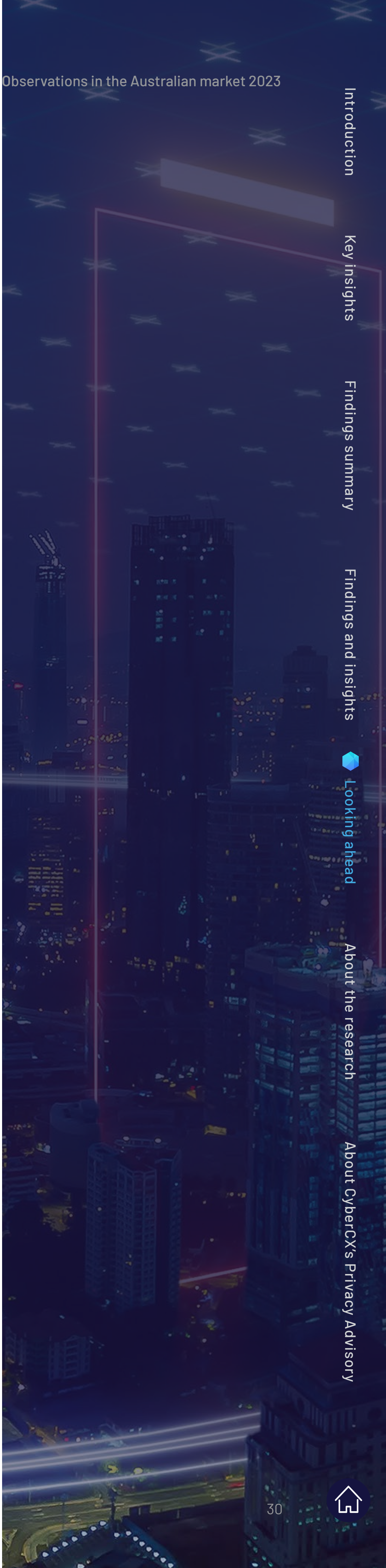
- the 'fair and reasonable' test
- enhanced consent requirements, and
- stricter requirements for activities that attract high privacy risk, such as direct marketing and the trading of individuals' personal information, and the use of artificial intelligence and automated decision making.

If adopted, we will likely see new privacy rights introduced, such as:

- the right to erasure
- objections to the collection of personal information
- right to de-index online search results, and
- right to a direct right of action for privacy breaches.

Backed by a new privacy penalty regime that will see organisations face significant penalties for privacy breaches, organisations will need to do more to build in new requirements into their governance, processes and systems to ensure they are prepared and ready for such changes.

By taking a Privacy by Design approach, organisations will be able to assure that privacy is respected and potentially go beyond privacy compliance requirements.



As raised throughout this report, the privacy risk and regulatory landscape has changed significantly in the last few years, thereby creating new threats and on the flip-side, new opportunities. Considering these seismic changes, CyberCX encourage:

Leaders and executives to consider the following questions:

#1 *What changes are anticipated as part of privacy law reform and how can my organisation prepare itself to meet these changes?*

#2 *What is the scale of activities my organisation requires to comply with key privacy reforms that will affect our business?*

Managers, privacy officers and other staff that have a role in handling personal information to consider the following questions:

#1 *Do I have full visibility over the data that my organisation collects, processes, discloses and stores? For example, do I know what kind of personal information my organisation holds across the digital ecosystem?*

#2 *What privacy and security controls does my organisation have in place to manage this information? For example, in relation to the data retention and destruction of data.*

About the research

The team

CyberCX's Privacy Advisory and Security Testing & Assurance practices collaborated to analyse the privacy and security practices of leading consumer brands operating in Australia.

Methodology

CyberCX's research consists of several stages, culminating in this report.

Brand selection

CyberCX identified 9-10 leading consumer brands with digital 'shopfronts' across 11 industry sectors operating in Australia based on:

- external brand value rankings
- web-traffic analysis, and
- external market share/valuation indexes.

Data collection, testing and analysis

CyberCX undertook a qualitative and quantitative analysis of brand's website applications to assess for:

- good privacy and security practices *e.g. comprehensive, easy to understand privacy notices and positive consent practices*
- negative privacy and security practices *e.g. the existence of privacy 'dark patterns' and the prevalence of tracking technologies.*

Our analysis was conducted on publicly available information, design characteristics and technologies found on brands' web applications. We undertook a combination of manual reviews, sampling, technical testing of security configurations using Open WPM[5], and Qualys SSL Labs APIs to test for the SSL/TLS configurations of the web servers.

Research metrics

Each of the seven Privacy by Design principles lends itself to measurable privacy and security attributes that can be found in the main digital interfaces of brands. Using

CyberCX's privacy, security and cyber-risk expertise we developed over 130 metrics for different features of brand web platforms. Web platform features included, among others:

- the user-interface for accessing or interacting with privacy related functions
- privacy documentation such as privacy policies, notices, cookie policies, and terms and conditions, cookie banners, pop-ups, consent mechanisms and privacy dashboards
- tracking technologies such as canvas
- fingerprinting, pixels, and third-party cookies etc.

Scoring method

We developed a scoring methodology that captures the estimated likelihood of a positive or negative privacy impact for each metric. Individual metrics were then assigned to a given Privacy by Design principle. Aggregates of metrics scores for each principle were then normalised to produce net Privacy by Design scores between 0 and 1. Collectively, these processes resulted in four kinds of scores:

- raw positive scores for each principle
- raw negative scores for each principle
- net scores (sum of positive or negative) for each principle
- normalised scores net scores[6].

The outcome is that brands were assigned increasingly positive scores for good privacy and security practices, and increasingly negative scores for potentially harmful privacy and security practices.

Limitations

The review of the brands was limited to public facing applications and privacy practices. CyberCX did not have visibility into the reviewed brands' internal data practices and systems, and as such, the commentary and scoring are based solely on publicly observable practices – the public consumer perspective.

OpenWPM was not used to analyse brand performance in authenticated environments. For example, OpenWPM was not used to assess the operation of ad trackers when an individual logs into their bank account. Accordingly, outputs of the OpenWPM analysis do not reflect the full breadth of information management practices users may be subject to across the entirety of their customer journey.

In some cases, the presence of certain features or properties of websites captured by OpenWPM do not necessarily entail poor privacy practices. For example, keyloggers can be used to invade privacy by capturing what individuals write on websites, however, they can be used to identify potential fraud when entering passwords when accessing sensitive environments such as bank accounts. CyberCX did not assess whether brands used certain potentially privacy invasive information to actually invade the privacy of individuals.

The seven Privacy by Design principles are not conceptually discrete and overlap considerably. Accordingly, assignment of metrics to principles is, to a significant degree, bound to the preferences and expertise of the assessors. For example, the presence of a high-quality cookie banner on a website could be seen as a representation of the proactive principle insofar as it can prevent privacy invasive practices before they happen, it could also be representative of privacy by default if the banner had cookies turned off by default. Where possible we have tried to break down such conflict by measuring discrete aspects of a given feature and assigning each one of those qualities to the right principle.

About CyberCX's Privacy Advisory practice

Privacy builds trust. Trust builds opportunity.

Management of privacy risk and obligations are increasingly being recognised by leading businesses as key to building sustainable and trusted market offerings and being an employer of choice. In the digital age, reputation is key and how you manage personal information can make or break your opportunities to grow.

CyberCX has experienced privacy practitioners who understand data, the opportunities it brings and the regulatory and social boundaries around its use. As data holdings grow exponentially and as business relies on a more complex web of service providers, understanding what is possible with data and what is required to manage privacy risk, means that intimate and deep knowledge of privacy is essential. From building a strategy through to controls that will help you manage and monitor your risk, our industry leading professionals will bring to your organisation decades of experience with some of Australia's and the world's largest corporations.

The Privacy by Design team 2023

The privacy experts and professionals who developed the CyberCX Privacy by Design research methodology and this report included:

David Batch
National Privacy Lead

Alex The-Tjoean
Privacy Manager

Jay Fradkin
Senior Privacy Consultant

Gabriella Assis
Privacy Consultant

Jeremy du Bruyn
Director, Security Testing and Assurance

Frikkie Jansen van Rensburg
Senior Security Consultant

Jacob Zimmermann
Senior Security Consultant

Natasha Ferguson
Marketing Manager

Linda Zhang
Senior Design Consultant

References

1. CyberCX note that, due to fact that this assessment focused upon publicly accessible features of web platforms, fewer metrics could meaningfully be deployed to measure the principle of Full Functionality compared to other principles.
2. HTTP Strict Transport Security (HSTS) is a policy mechanism that helps to protect websites against man-in-the-middle attacks such as protocol downgrade attacks and cookie hijacking.
3. Content Security Policy (CSP) is a computer security standard introduced to prevent cross-site scripting (XSS), clickjacking and other code injection attacks resulting from execution of malicious content in the trusted web page context.
4. Transport Layer Security (TLS) is an encryption protocol that provides end-to-end security of data that is sent over the internet.
5. OpenWPM is a web privacy measurement framework created to enable data to be collected on a scale of thousands to millions of websites for privacy studies. OpenWPM is built on top of Firefox, with automation provided by Selenium. CyberCX used the Mark-up's Privacy Blacklight, a customization of OpenWPM as part of this assessment.
6. Net scores were normalized for the purpose of making fair comparisons between net scores for each principle noting that a different number of metrics were assigned to each principle, there by producing different net scores for each principle (which are not directly comparable).

Are your websites or mobile apps 'Privacy Ok'?

Organisations regularly test their mobile apps and websites for security vulnerabilities, but when was the last time you checked for privacy compliance?

Since December 2022

The maximum fines for a privacy breach have risen considerably, alongside an increasing expectation from the community that privacy is protected.

Organisations need to be sure

That their apps and websites are consistent with the law, the promises made in their privacy policies and with any consents given or withheld.

The annual CyberCX Privacy by Design research

Has given us unparalleled insights in the Australian market on what good looks like online, and where organisations fall short.

Our research consistently finds that websites and mobile apps often behave differently to what has been promised, such as:

- **collecting personal information** that is not called out in a privacy policy
- **collecting personal information** that is either not expected or required
- **using tracking technologies** that have not been consented to or are unknown to you
- **sending personal information** to third parties without the appropriate consents and safeguards in place.

*Our market leading combination of expert **privacy advisors** and **security testers** can provide assurance that your mobile apps and websites are not creating unnecessary privacy risk for their users and your organisation.*

Contact us to find out more at:
privacyadvisory@cybercx.com.au

CyberCX

1300 031 274
cybercx.com.au
info@cybercx.com.au

CyberCX Pty Ltd
Level 4, 330 Collins Street
Melbourne, VIC 3000, Australia
ABN: 90 629 363 328