



CyberCX
Privacy by Design

Observations in the Australian Market 2022

**Beyond minimum compliance,
towards a privacy and customer
centric approach**

Contents

Introduction	3/
About the research	4/
Key insights	6/
Executive summary	9/
Findings and insights by Principle	11/
Looking ahead	28/
About CyberCX's Privacy Advisory Team	29/



Privacy by Design – Observations in the Australian Market 2022

CyberCX's Privacy by Design – Observations in the Australian Market Report is the first edition of the analysis of over 100 top consumer brands operating in Australia and their performance against the 7 Privacy by Design Principles, to uncover what brands are doing to demonstrate excellence in Privacy by Design.

Introduction



Community awareness of privacy risk in the digital age is ever-growing given increasing notification of data breaches, media attention on questionable data practices and regulatory changes occurring around the world. This means that how a brand approaches privacy is becoming more than just a legal or compliance issue but increasingly, a reputational, business and financial risk – **or opportunity**.

Privacy 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 risks increase against a complex regulatory landscape.

The 7 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 incorporated 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 eleven industry sectors have embedded Privacy by Design into their primary web-based customer and user interfaces.

Assessing over 140 unique attributes, each aligned to one of the seven Privacy by Design Principles, we've measured the publicly available features of each brand's web application including privacy attributes, and technical security capabilities that generate **positive and negative** privacy impacts. Using a proprietary scoring methodology applied to each of the negative and positive privacy attributes, we've been able to determine how each of the industry sectors have performed in embedding Privacy by Design in their digital shopfronts.

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 harness the power of personal information for the benefit of all and build consumer trust.

“

Privacy by Design takes the view that the future of privacy in a digitally driven society cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organisation's default mode of operation. ”

Office of the Privacy Commissioner,
New Zealand

About the research



The team

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



Methodology

Brand selection

CyberCX identified 10-20 leading consumer brands 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 found on brands' web applications. We undertook a combination of manual reviews, sampling, technical testing of security configurations using Open WPM, and Qualys SSL Labs APIs to test for the SSL/TLS configurations of the web servers.

Research metrics

Each of the 7 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 145 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 and privacy dashboards
- ▶ tracking technologies such as canvas fingerprinting, pixels, and third-party cookies etc.

Aggregates of metrics were then uniquely assigned to different privacy by design principles to produce privacy by design scores.

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 selected for assignment to a given Privacy by Design Principle to produce a total score for a given principle. This resulted in four kinds of scores:

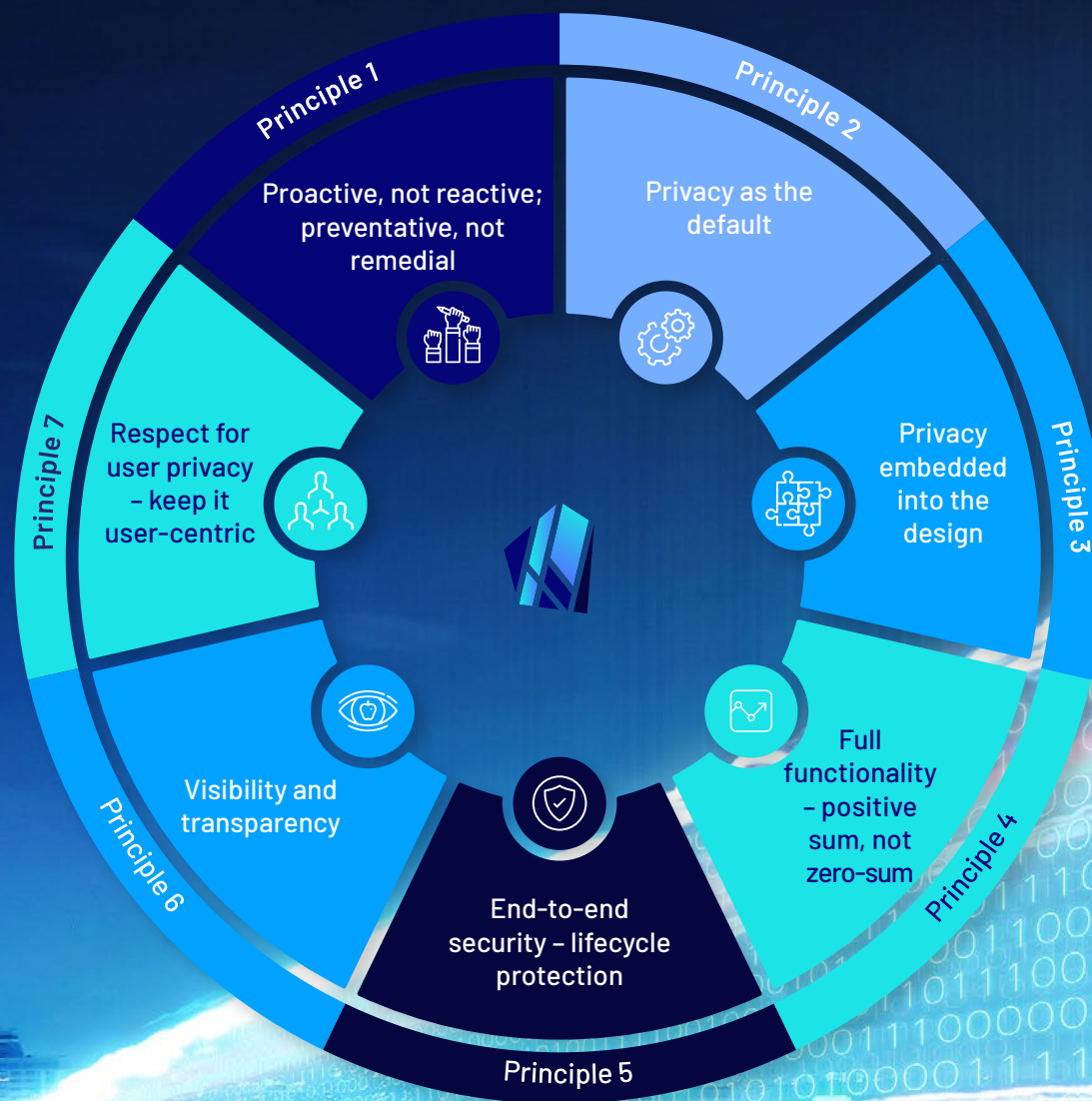
1. Raw positive scores for each principle
2. Raw negative scores for each principle
3. Net scores (sum of positive and negative) for each principle
4. Normalised net scores

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

To produce the insights for this paper, we aggregated the the brand-level data collected to produce overall industry scores.

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 145 different and measurable attributes, each of which maps to one of the 7 Privacy by Design Principles.







Key insights



This year's Privacy by Design – Observations in the Australian Market report highlights that while several sectors performed better than their peers in upholding the 7 Privacy by Design Principles in their digital interfaces, with Telecommunications & Technology, Banking & Finance and the Government sectors leading the way, there are significant opportunities for improvement across the board.

Overall top 5 performing sectors

- 1 Telco & Technology** 
- 2 Banking & Finance** 
- 3 Government** 
- 4 General Insurance** 
- 5 Transport & Travel** 



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 Telco & Technology sector developed and published Privacy Principles that guide in the design of their products and service offerings, and published advice to consumers on privacy and cyber security.



Principle 2: Privacy as the default

Good practices observed include accessed services and cookie banners not having the most permissive privacy settings by default, and the availability of opt in/out settings. Leading brands were found in the Government sector.



Principle 3: Privacy embedded into the design

Brands that performed well made it easy for users to exercise their privacy rights through the use of privacy dashboards and cookie banners that facilitated meaningful control of user's privacy settings. Leading brands were found in the Transport & Travel, Telco & Technology, and Government sectors.



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

Strong performance was achieved by brands that balanced seemingly opposing interests, such as security and privacy. Leading brands were found in the Food & Grocery, and Telco & Technology 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 Telco & Technology and Social Media sectors.



Principle 6: Visibility and transparency

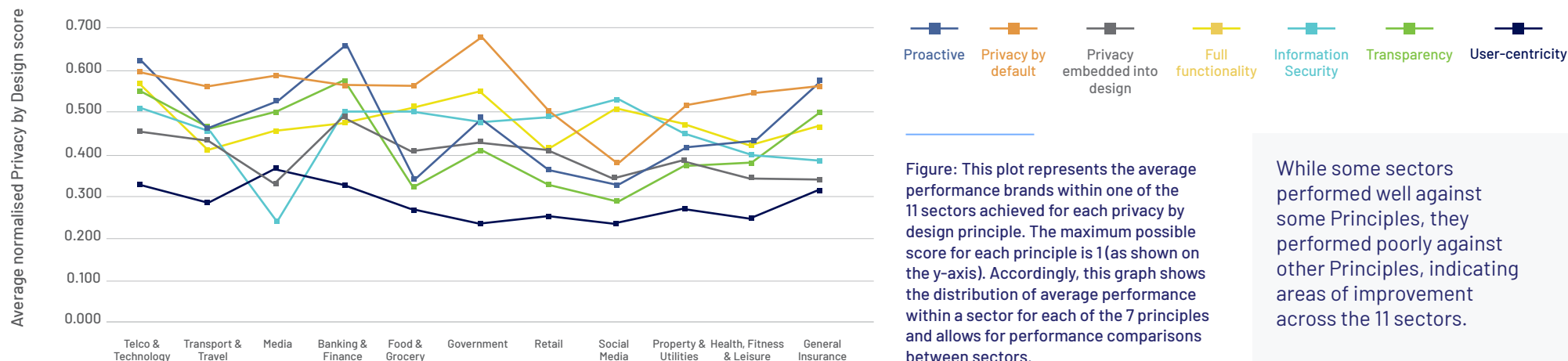
Strong performers made the overall presentation of privacy related information, privacy features and easy and clear to understand. Notable practices brands engaged in include publishing their Privacy Management Plan. Leading brands were found in the Banking & Finance and General Insurance sectors.



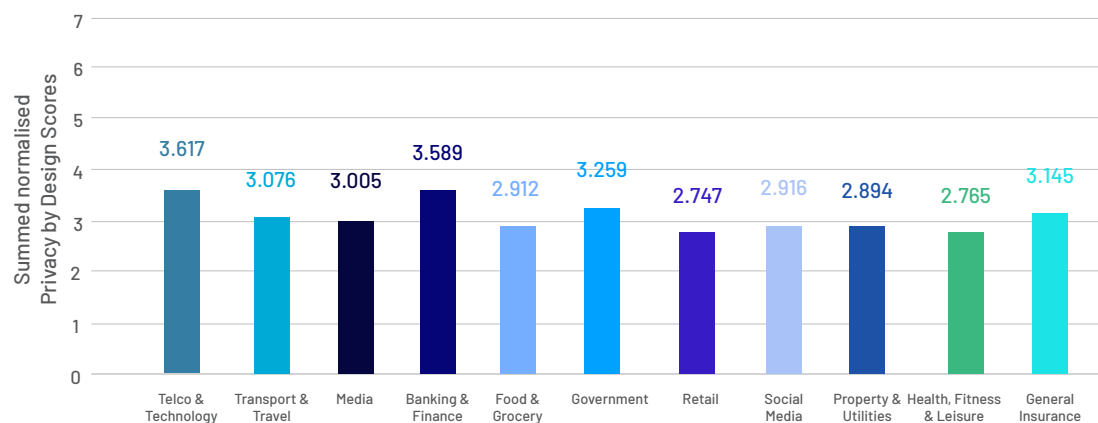
Principle 7: Respect for user privacy – keep it user-centric

Brands that performed well designed their platforms for user privacy. Leading brands come from the Media, General Insurance and Telco & Technology sectors.

Average normalised Principle score by sector



Net Privacy by Design score by sector



“ 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. ”

Office of the Australian Information Commissioner

Privacy by Design is built around 7 key Principles.

By applying these Principles into the design of your applications, systems, products and business processes, privacy can become a point of differentiation for organisations that want to achieve a competitive business advantage.

By implementing a “Privacy by Design” approach, organisations can:

- ▶ build consumer trust and confidence through protecting user’s privacy online
- ▶ go beyond minimum compliance with legal and regulatory obligations, and
- ▶ reduce overall privacy and cyber-risk for their organisation.

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

The Telco & Technology sector performed the strongest overall across all 7 Privacy by Design Principles. This was achieved through several positive privacy practices by the brands in this sector, including by publishing privacy and security blogs posts, and minimising the use of negative practices which result in ‘reactive’ approaches to privacy management. Other sectors with the most outstanding individual brands were in the Banking & Finance and Governments sectors, many of which have taken proactive measures to implement Privacy by Design.

Good practices observed

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

- ▶ turned privacy into a competitive business advantage by taking a privacy by default approach to their communications and designing their products
- ▶ designed customer interfaces for user transparency and trust, taking proactive steps to meaningfully inform users about how they were handling user’s personal information, and
- ▶ made user privacy management easy, by developing user-centric privacy dashboards that provide users with greater control over their personal information.

Areas for improvement

The brands that performed the worst:

- ▶ had poor Privacy Policies in place that did not meet legislative privacy requirements, performed poorly on readability tests, and were less accessible to users
- ▶ 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 than the average brand.

Australian privacy law reform

While several brands performed well, CyberCX's findings reveal that significant areas of improvement exist for brands across sectors in their openness and transparency of personal information handling practices, notice and consent practices, default privacy settings, use of tracking technologies and existence of dark patterns.

In our constantly evolving digital environment, it is unreasonable to expect everyday Australians to be able to protect their personal information, and anticipate the myriad of cyber risks that exist, given the power imbalance that exists between organisations and individuals. Shifting the onus away from individuals and towards organisational accountability, the Australian Government should employ an accountability-based privacy model. As custodians of data, this would see that organisations are charged with the responsibility to

use personal information in a manner that is fair and reasonable, protects against individual and collective privacy harms, and promotes consumer trust and confidence.

This could be achieved by introducing:

- ▶ an accountability requirement for organisations regulated under the Privacy Act to implement "privacy by design and default," across the Australian Privacy Principles (APPs). This is similar to the approach taken in the European Union with the General Data Protection Regulation, and
- ▶ strengthened requirements for personal information handling practices across the APPs – for example through enhanced transparency, data collection and consent requirements.



Findings and insights

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.

Insights:

The 11 sector's performance ranked:

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

In practice...



Privacy strategy

Make data privacy a strategic priority and have a well-defined Privacy Strategy



Privacy awareness and education

Educate users about your organisation's data practice and maintain transparency



Empower your customers

Be privacy and customer-centric by empowering users with real choice over how their personal information is handled

Did you know?

Over 50% of Australians experienced a problem with how their data was used, such as unwanted marketing communications, or personal information being collected when it was not required.

Source: The Office of the Australian Information Commissioner, Australian Attitudes to Privacy



Case studies

Designing for privacy and trust: leading with privacy principles

Taking a proactive approach to privacy, four brands have sought to make privacy a business advantage. These brands have developed and published privacy principles to guide them in their communications, and the design of products and services. Some of these principles include data minimisation, user transparency and control, choice, and security.

Enhancing transparency and empowering users

One brand from the Telecommunication & Technology sector produced "A Day in the Life of Your Data" report to illustrate how third-party companies track user data across websites and apps. The report shares the privacy features available across the brand's products to provide users with more transparency and control, empowering individuals with the knowledge and tools to control their personal information.

FINDINGS

Average scores by sector for the Proactive Principle

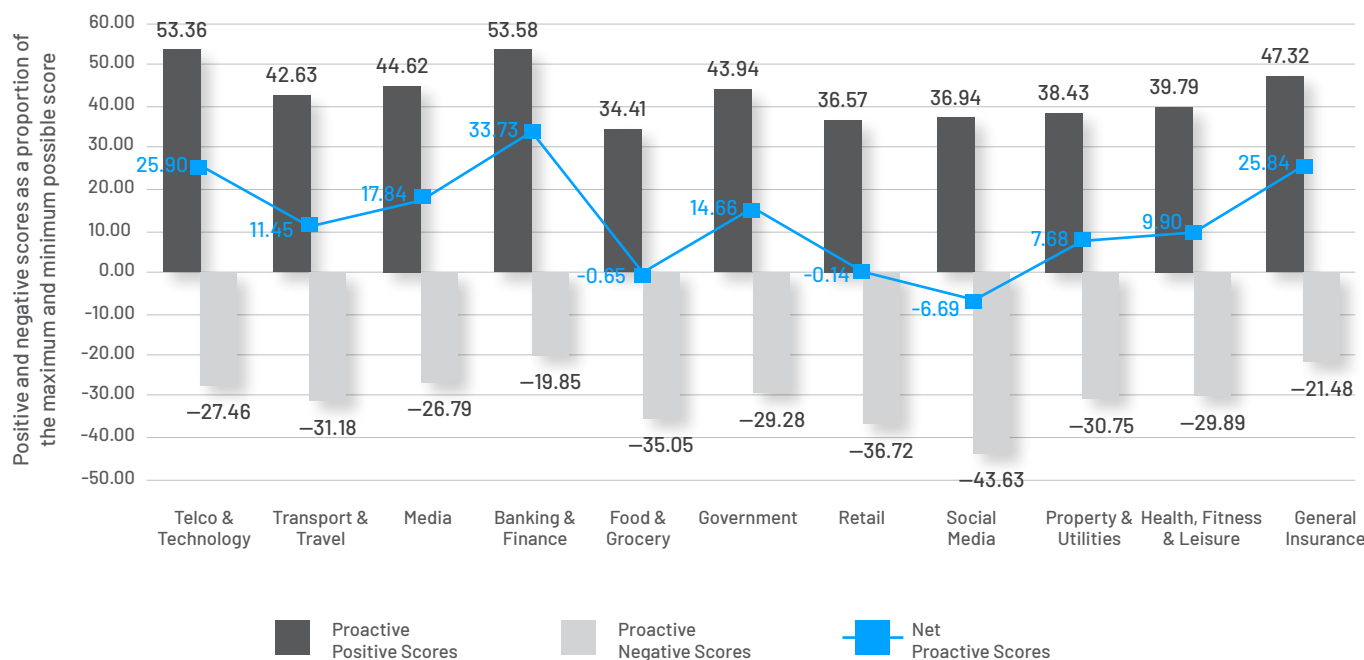


Figure: This plot shows the distribution of average positive and negative scores achieved by each sector. Sector positive scores are represented by the dark grey bars which reflect the average proportion (percentage) of the maximum possible positive score achieved by each sector against the Proactive principle. Negative scores are represented by the 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 these positive and negative scores. This description applies to all following plots.



Results

Overall best performers

The Banking & Finance sector reflected the strongest overall embodiment of this Principle out of the 11 sectors tested.

Worst performers

The Social Media, Retail, and Food & Grocery sectors produced largest net negative average scores against this Principle.

Areas for improvement

Brands could undertake several measures to adopt a proactive approach to privacy, such as by informing customers of the Privacy Principles they abide by when designing their products.

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.

Insights:

The 11 sector's performance ranked:

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

In practice...



Data minimisation

Minimise data collection to what is necessary. Don't collect data for the sake of collection or because you can



Marketing and tracking

Have marketing and tracking technologies switched off by default, asking customers and users to opt-in



Security

Implement appropriate technical security measures, such as encryption to ensure the confidentiality, integrity and availability of personal information

Case studies

Cookies and tracking technologies off by default

All brands deploy some form of tracking technology on their web platforms. Importantly, not all tracking technologies are equal when it comes to their privacy invasiveness. Some tracking technologies, such as short duration first-party cookies, can improve user experience by temporarily storing information about user-selected preferences while minimising privacy impacts. None of the surveyed brands stored first-party cookies for more than 90 days, which is a positive privacy practice because the websites are

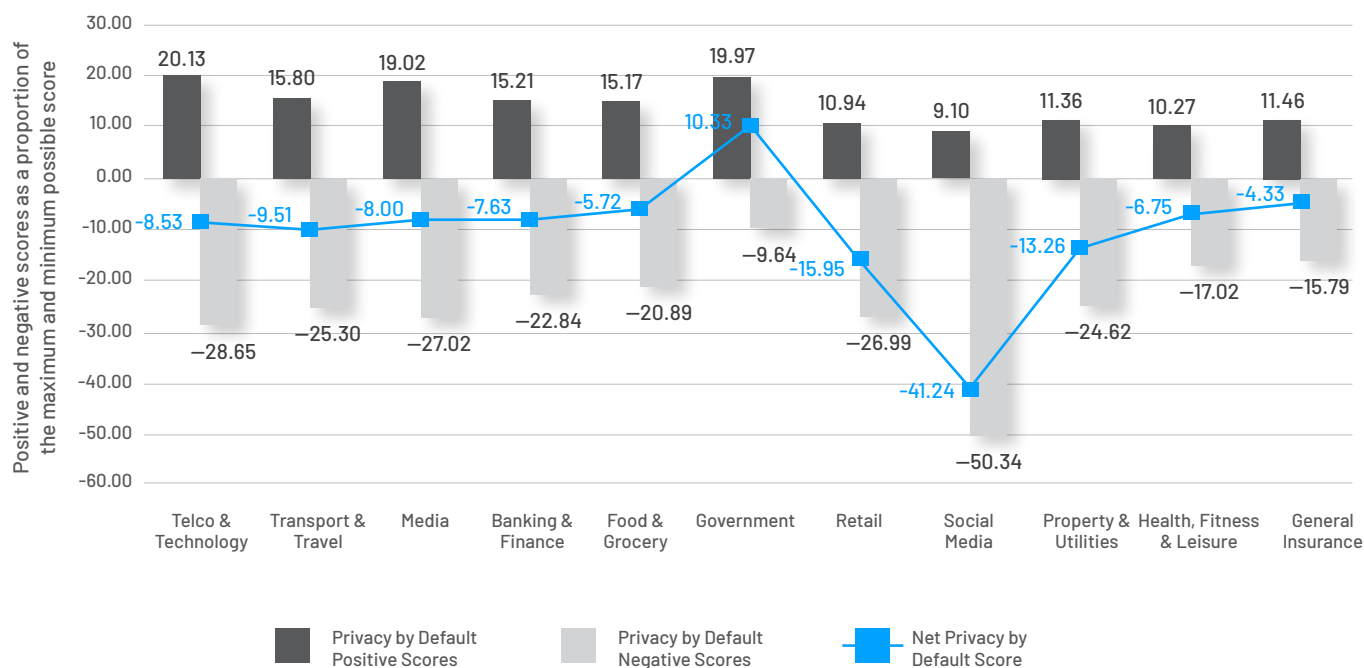
not storing store user-generated data longer than would be reasonably necessary for their business functions.

Other tracking technologies, such as third-party cookies can be more privacy invasive. Brands face a privacy trade-off when using these technologies. This is because they can be deployed to monetise users in some capacity, whether it be profiling customers for targeted advertising, or selling user activity information. Third-party cookies are technologies which collect information about a user's interaction with a web platform that are operated by entities other than the owner of web platform the user is

visiting. More third-party cookies operating on a website means that the website you're visiting is sharing the information you create with more entities. On the flip side, the fewer third-party cookies operating a given web platform means that, overall, the website provides stronger privacy protection by default. 1 in 4 brands surveyed minimised the number of third party cookies operating on their platform to three or less. This means 3 in 4 brands could strength their privacy by default settings by reducing the amount of information they share with other entities about user activities on their websites.

FINDINGS

Average scores by sector for the Privacy by Default Principle



Results

Overall best performers

The Government sector produced the strongest overall Privacy by Default Principle scores out of the 11 sectors tested. This score was achieved, in part, by implementing the principle of data minimisation when collecting personal information.

Worst performers

The Social Media platforms produced the lowest score by affecting practices which required the collection of personal information from individuals where there were few controls in place to allow individuals 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.

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 **54 out of 100** brands loaded at least 7 or more advertising trackers on their web platforms. Of those 54 brands, 20 of those brands loaded over 15 ad trackers on a webpage.

Ad tracking technologies load JavaScript codes or invisible images that can be used to identify and profile users for ad targeting purposes. The more advertisement trackers operating on a web platform, the more collected information is disseminated to different entities across the internet.

Third-party cookies

CyberCX found that **26 out of 100** brands loaded three or less third-party cookies. 49 out of 100 brands loaded 10 or more third-party cookies on their webpages.

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 **85 out of 100** brands used canvas finger printing and 95 out of 100 brands use canvas font 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.

Session recording services

CyberCX found that **70 out of 100** 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 Markup, research has shown that these practices are insecure and create sensitive user data.

Keystroke capturing

CyberCX found that **87 out of 100** brands used some form of keyloggers. CyberCX did not determine whether these keyloggers were deployed for legitimate or malicious purposes.

Keystroke capturing, or keylogging is when a website uses software to record some or all of what you type on the website. Websites can use keylogging for legitimate purposes, however, they can be used to quietly monitor your computer activity while you use your device as normal. As with session recording, keylogging can increase security risks for users, particularly if things like passwords and usernames are recorded.

Facebook pixels

CyberCX found that **38 out of 100** 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.

Google Analytics

CyberCX found that **69 out of 100** 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.

Privacy embedded into the 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.

Insights:

The 11 sector's performance ranked:

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

In practice...



Embed Privacy by Design

Embed privacy into the design of web and mobile applications, technologies, and systems to the greatest extent possible, without impairing their functionality



Use, retention and disclosure limitation

Don't collect data for any other purpose than which the user has agreed, and don't keep data after it's no longer needed



Cookie banner

When using cookie banners, ensure users are able to easily opt-in and out

Case studies

Cookie Banners

A cookie consent banner is a notice that is displayed on websites and other apps when a user first visits a website. Its function is to provide information about the use of cookies, and to provide the user consumer rights by creating an opportunity to give or deny consent to activate site cookies. Cookie banners can be a good mechanism for brands to embed privacy features into the design of their websites.

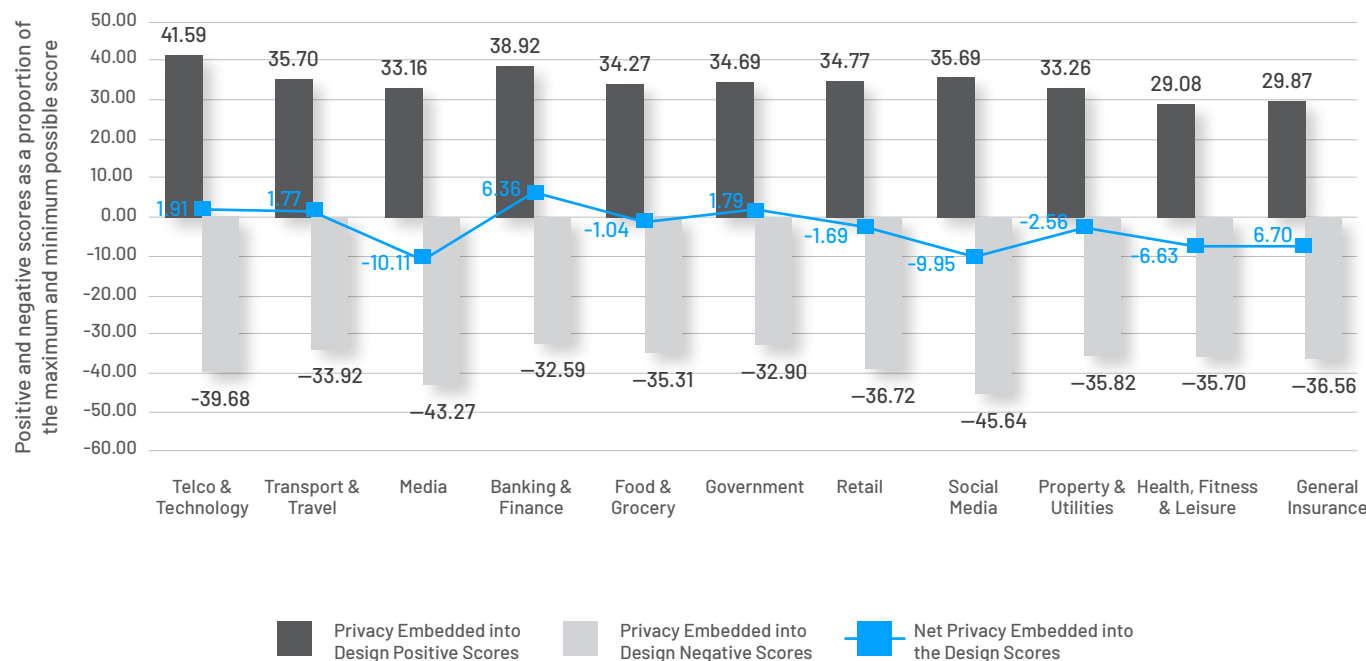
In some jurisdictions around the world, such as countries bound by the European ePrivacy Directive, it is mandatory for websites to display a cookie banner. However, it is not mandatory for Australian brands to have a cookie banner on Australian-based websites. CyberCX found that only 10% of surveyed brands

presented a cookie banner to users when accessing their websites.

Importantly, presentation of a cookie banner alone does not necessarily represent a positive implementation of the principle of embedding privacy into the 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 thereby creating an illusion of choice. CyberCX found that only 4 out of the 10 websites that had a cookie banners presented the banner with the most privacy protective settings as the default option. Thus, an important lesson is for brands to not only have cookie banners in place, but to design them in a way which protects and promotes user privacy.

FINDINGS

Average scores by sector for the Privacy Embedded into the Design Principle



Results

Overall best performers

There was relatively consistent performance across the 11 sectors in Privacy Embedded into the Design with Banking & Finance being the top performer. For example, the Banking & Finance sector typically did not allow long duration (>90 day) third-party cookies to be built into and operate on their web platforms.

Worst performers

The Media sector produced the lowest average score, achieved in part due to the use of keyloggers on their web platforms.

Trends across all sectors

On average brands affected a range of practices which promoted Privacy by Default, however, this was counter balanced by other practices.

Areas for improvement

In general, a range of practices relating to the online profiling, tracking and monitoring of users activities on web platforms counterbalanced other positive activities affected across each sector. Brands could improve their privacy posture by seeking alternate opportunities to generate profits than by tracking user activities online.

Full functionality: positive sum, not zero-sum

What is this Principle about?

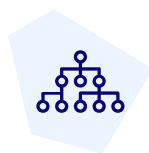
Organisations that take a positive-sum, “win-win” approach integrate privacy with other legitimate objectives and interests, such as security or user experience – this avoids trade-offs or limitations on functionality from occurring should users want to share less personal information.

Insights:

The 11 sector's performance ranked:

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

In practice...



Enable full functionality

Find solutions that enable multi-functionality so that legitimate interests and objectives can be achieved

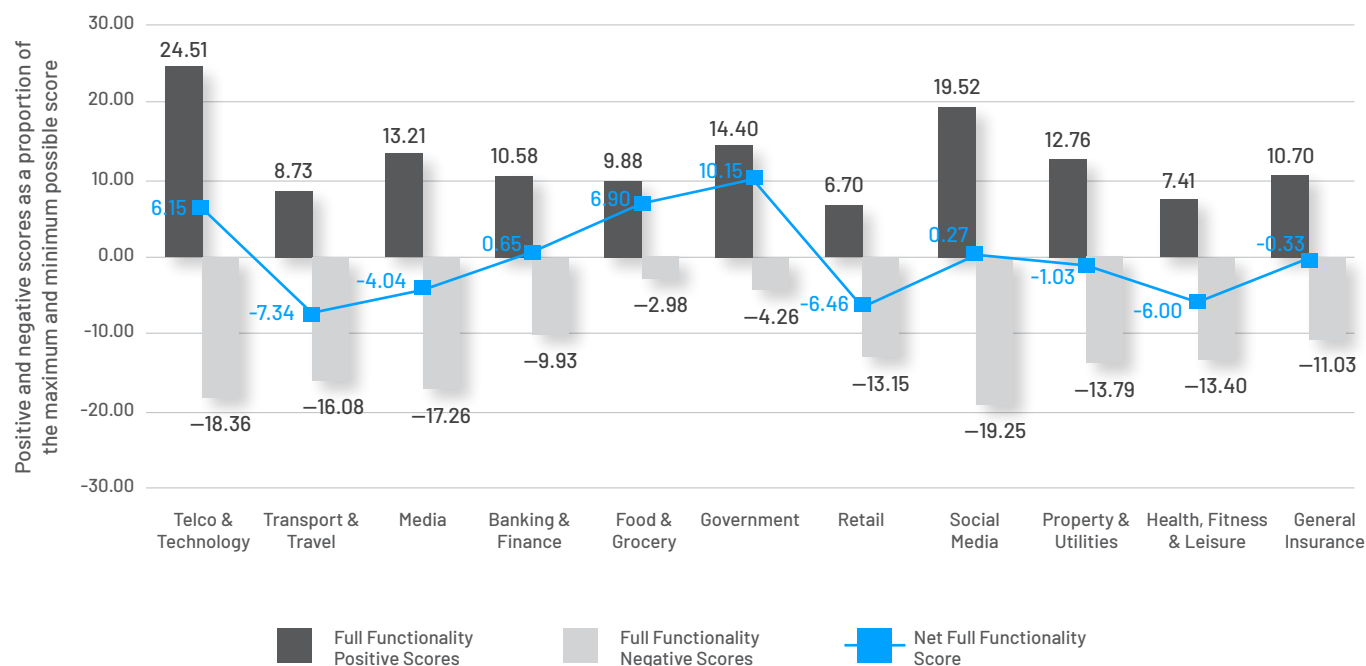
Case studies

Functionality at the cost of your personal information

One example of Full Functionality in practice is whether 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. The opposite of full functionality, in this case, is where the price of accessing an otherwise free feature or service (i.e. getting full website functionality) is the provision of your personal information. Many users will be familiar with the experience of wanting to read a report on a website, only to find you have to provide your email and other personal details for marketing purposes to access the report. CyberCX found that approximately 2/3 of websites surveyed do not engage in practices where the price of full functionality is the provision of your personal information. This represents a positive step in the right direction for full functionality with some room for improvement.

FINDINGS

Average scores by sector for the Full Functionality Principle



Results

Overall best performers

The Government sector performed strongly in the Full Functionality category, in part, by allowing users to access web platform features and services without having to register and provide personal information for superficial encounters.

Worst performers

The Retail and Transport & Travel sectors were closely matched in terms of scores. This is in part due to the requirement for individuals to provide more information than is strictly necessary when accessing web platform features, goods and services.

Trends across all sectors

In general, most brands required the collection of personal information when accessing services when the requirement, or breadth of information collected may have not been necessary for the functions users sought to access.

Areas for improvement

An area where many brands could boost website 'full functionality' is by providing open and free access to website services and features without registration requirements, where it is not strictly necessary for the user to register with the platform to use its services.

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.

Insights:

The 11 sector's performance ranked:

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

In practice...



Security

Implement appropriate technical security measures, such as encryption to ensure the confidentiality, integrity and availability of personal information



Data retention

Define data retention periods for the user data you hold; indefinite retention is never acceptable

Case studies

Login and device access history

27 brands provide users with an overview of recent security activity, such as new sign-ins from unknown devices or locations. When a new sign-in occurs, some brands notify users directly, enabling users to verify the activity in real time. Providing users with security tools like this can help users audit their own account activity and to recognise a security compromise early.

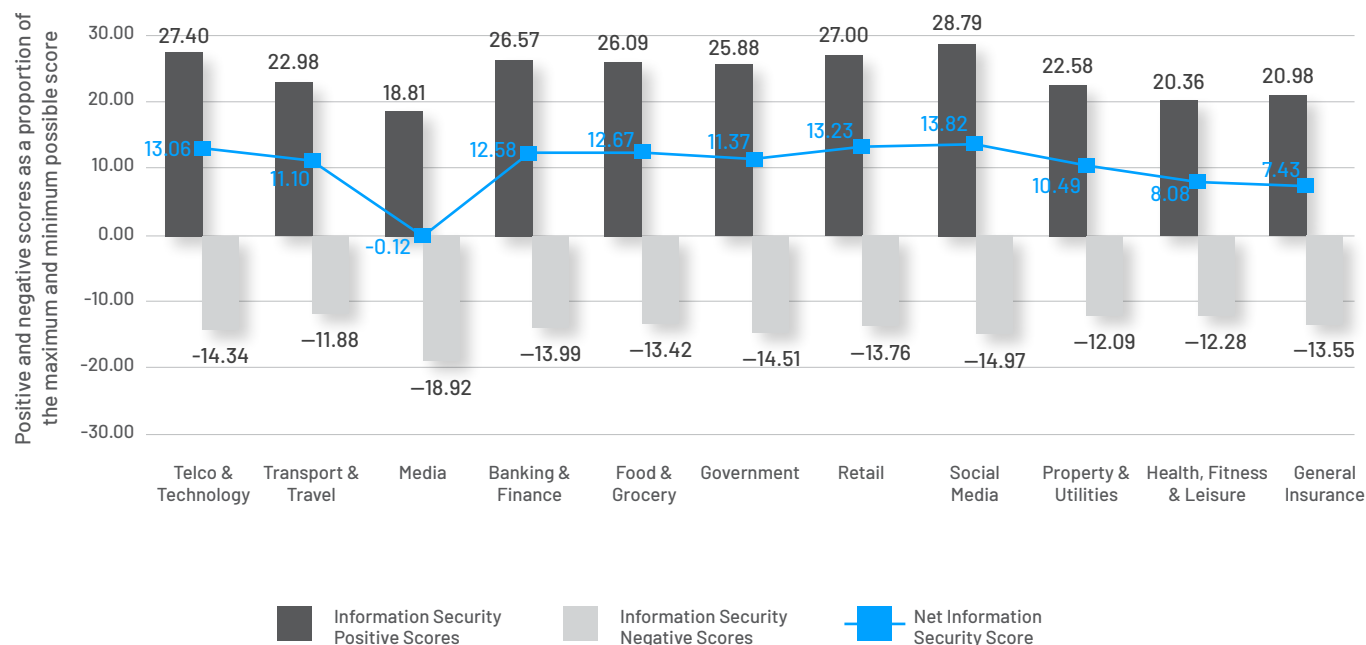
Using Multi-Factor Authentication by default

34 brands offer some form of two factor authentication to their users. 11 of those brands enable the feature by default. Two factor authentication provides an extra layer of verification for users and can mitigate the risk of unauthorised access to the user's personal information. Making this feature available by default ensures that all users benefit from the same minimum level of protection regardless of the user's cyber security awareness.



FINDINGS

Average scores by sector for the Information Security Principle



Results

Overall best performers

Overall, 6 sectors were closely matched in averaged security metrics with the remaining 5 sectors lagging slightly behind. Positive scores were due to affecting positive practices such as achieving an A+ rating for Qualys SSL Labs analysis of a given web platforms and Transport Layer Security (TLS) protocol configuration. Other positive practices included not using third-party cookies and tracking technologies such as advertising trackers, canvas fingerprinting, and engaging in session recording.

Worst performers

The Media sector underperformed compared to other sectors due to widespread use of session recording, failure to enforce HSTS and secure first-party cookies.

Trends across all sectors

Overall, all sectors produced the most consistently high performance for the information security principle compared to other Privacy by Design Principles. This demonstrates that brands take high level, publicly accessible features of the information security performance of their websites seriously.

Areas for improvement

Brands could focus on removing the use of tracking technologies that pose information security and privacy risks, such as keyloggers as well as ensure the currency of TLS configuration across their web platforms.

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 what they're doing.

Insights:

The 11 sector's performance ranked:

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

In practice...



Openness and transparency

Information about your data practices, and privacy policies and procedures should be openly available to individuals

Did you know?

The ACCC's Digital Platforms Inquiry found that many customers are not aware of how digital platforms collect, use and share their data, including for targeted advertising and online profiling purposes. Information asymmetry is sustained through long, complex, and vague terms of use and privacy policies.

Source: Australian Competition & Consumer Commission, Digital Platforms Inquiry



Case studies

Accessibility and readability of privacy policies

Every brand surveyed had a privacy policy and the vast majority of brands (95/100) made their privacy policies easily accessible by placing hyperlinks in obvious locations on their web pages e.g. at the bottom of the page where other administrative functions are located.

The privacy policies of nine brands had Flesch Kincaid readability scores over 70 which means that they should be easily understood by the average 7th grade student. Enhancing the reading ease of privacy policies increases the chance that their content will be understood by a wider audience, thereby uplifting the transparency of brands information handling practices to more people.

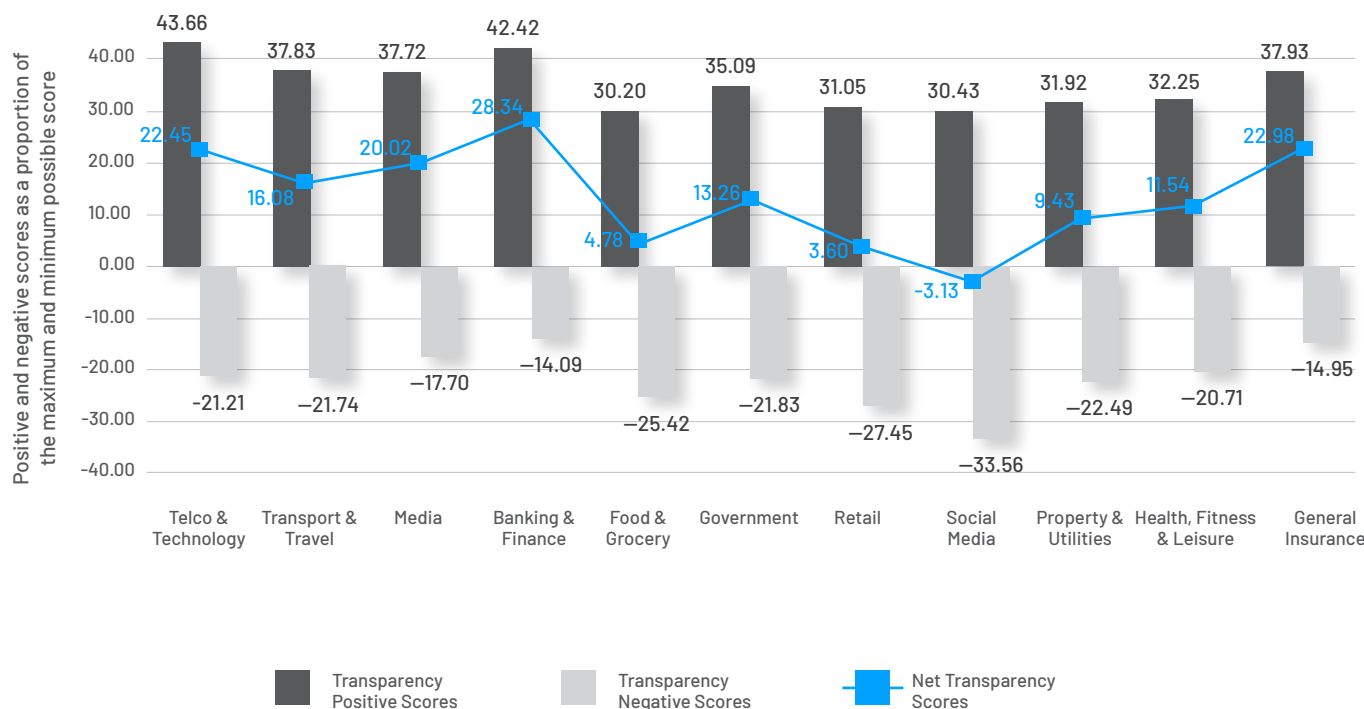
In addition, 12 brands also offered their privacy policies in languages other than English which further increases the accessibility of information about personal information management practices.

Privacy promotion

Almost one third of brands affected visibility and transparency best practice by providing users with more accessible and digestible privacy information to promote accountability and trust. For example, these brands published privacy and cyber security blog posts or articles to educate users about their activities in these spaces

FINDINGS

Average scores by sector for the Transparency Principle



Results

Overall best performers

The Banking & Finance sector were the top performers overall with General Insurance, and Telco & Technology closely behind. Positive performances were due in part to comprehensive, layered, and accessible privacy policies and notices.

Worst performers

The Social Media sector consistently produced lower scores on average due to factors such as low Flesch readability scores for their privacy policies and a lack of clear, appropriately detailed privacy notices. These factors may impact the degree to which users are made aware of social media platforms intentions and practices regarding their data collection and personal information handling practice.

Trends across all sectors

Overall, 5 out of the 11 sectors demonstrated stronger commitment to the Principle of Transparency by providing users with comprehensive, accessible privacy policies.

Areas for improvement

An area for improvement for most sectors relates to the readability of privacy policies. Ensuring that privacy policies contain clearly articulated, simple language will ensure that relevant privacy information is available to the broadest possible audience, including children.

Respect for user privacy – keep it user-centric

What is this Principle about?

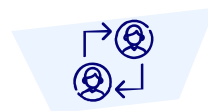
To ensure user-centred privacy, organisations can implement safeguards and features that make privacy management easy. This includes by using strong privacy defaults, meaningful notices, and user-friendly options and controls.

Insights:

The 11 sector's performance ranked:

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

In practice...



User-friendly controls

Provide users with meaningful choice and control about how their personal information is handled



Meaningful user choice

Avoid pre-ticking checkboxes which steal away the choice a user may exercise

Did you know?

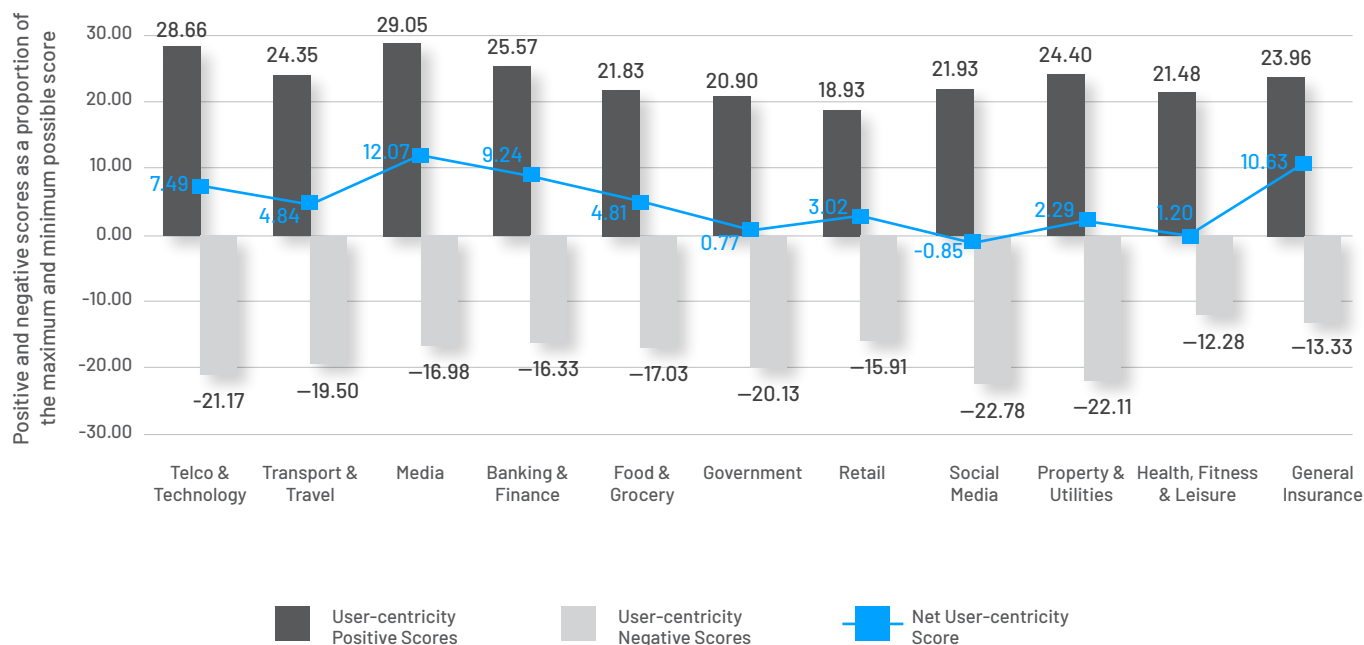
The ACCC's Digital Platforms Inquiry found that digital platforms' user interfaces lead consumers to make privacy-intrusive choices by appealing to certain psychological or behavioural biases. Some digital platforms used pre-selections and privacy intrusive defaults which resulted in information being presented in certain ways, such as reducing the visibility of problematic terms.

Source: Australian Competition & Consumer Commission, Digital Platforms Report 2020



FINDINGS

Average scores by sector for the User Centricity Principle



Results

Overall best performers

The General Insurance and Media sectors produced the highest overall average scores against this Principle. These sectors performed well by demonstrating 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

Five of the 11 sectors surveyed produced consistently lower average scores overall due to challenges around the ease with which individuals could access information about the brands personal information management practices. Brands also consistently omitted user controls around the operation of third-party cookies on their web platforms.

Trends across all sectors

Overall, most Australian based websites did not provide users the option to control what cookies, tracking technologies and analytics technologies operated on their web platforms.

Areas for improvement

The next step for the majority of Australian-based web platforms is to implement the principle of respect and user-centricity by providing users with controls regarding the operation of cookies, tracking technologies and analytics technologies on their digital interfaces.

“ Data protection by design is about considering data protection and privacy issues upfront in everything you do. It can help you ensure that you comply with the UK General Data Protection Regulation’s fundamental principles and requirements, and forms part of the focus on accountability. ”

United Kingdom Information Commissioner’s Office

As privacy expectations evolve, where users and consumers demand more protections and control over how their data is used, organisations will only be able to achieve this through taking a Privacy by Design approach. Compliance with law that is typically outdated the day it is enacted will not likely be enough to meet the market's demands.

Key questions leaders and executives should be asking:



1. How can you add privacy to your organisation's value proposition?
2. How are you reaching your privacy goals for 2022 and beyond?
3. How can you ensure that privacy becomes a core value across your organisation?

Key questions digital specialists, designers and architects should be asking:



1. How can you build "Privacy by Design" into your organisation's digital customer interfaces and applications, business practices, and products and service offerings?
2. What user-centric privacy controls and protections can be embedded into solutions?

About CyberCX's Privacy Advisory Team



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 2022

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

David Batch, Privacy Capability Leader

Alex The-Tjoean, Privacy Manager

Jay Fradkin, Senior Privacy Consultant

Sandra Raub, Privacy Consultant

Gianluca Muscas, Team Lead - Security Testing & Assurance

Jacob Zimmermann, Senior Security Consultant

Linda Zhang, Senior Design Consultant

“ (Privacy by Design) truly becomes a win-win.
I want companies to know that this is in their
best interests to do. ”

Dr Ann Cavoukian,
former Privacy Commissioner, Ontario



©2022 CyberCX Privacy Advisory
CyberCX Pty Ltd

Level 4, 330 Collins Street
Melbourne, VIC 3000, Australia

ABN: 90 629 363 328

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