



**Senate Economics References Committee
Inquiry into International Digital Platforms
operated by Big Tech Companies - March 2023**

Google Response

Introduction

Google welcomes the opportunity to provide this submission in response to the Senate Economics References Committee ('the Committee') inquiry into international digital platforms.

We provide responses below on some key parts of the Committee's issues paper.

Google's commitment to Australia

Google is committed to Australia and we believe that digital technology is critical in our nation tackling critical challenges, building our resilience and driving the economy.

In October last year, we released the 2022 edition of our [Economic Impact Report](#) prepared by AlphaBeta, highlighting key aspects of our commitment and the value of our impact on the Australian economy.

Using digital technologies to solve critical national challenges

The research by AlphaBeta examined three critical challenges facing Australia: digital skills shortages in the labour market, cybersecurity risks and the rise of climate change-caused natural disasters. It found that better utilisation of digital technologies across these challenges can help Australia gain up to \$56.7 billion in 2030, including:

- Reducing obstacles in the job search process and improving digital skills training, digital technologies can create up to an additional \$25 billion in GDP per year
- Deploying AI and secure cloud services, and educating the public about cybercrime prevention, can save business and consumers \$27.2 billion in annual losses, and
- Applying digital technologies in disaster response can mitigate up to \$4.5 billion in annual damage costs to property, crops, and livestock in 2030.

Google is helping to build Australia's resilience across these challenges through working across four key areas:

- **'[Digital Future Initiative](#)' (DFI): [launched in 2021](#)**, the DFI is a \$1 billion investment over five years to build a strong digital future for all Australians focused on three aspects: building secure and robust local digital infrastructure; launching Google's first Australian research hub leveraging AI and machine learning technologies; and, developing technology partnerships, like in the areas of sustainability and health.
- **Digital Training and Skills:** Google is committed to improving digital training and skills for Australians through:

- [‘Grow with Google’](#): under this program, we have provided free digital skills training to over 600,000 Australian small businesses and individuals, helping them to grow their presence online and thrive in the digital economy
- [‘Career Certificates’](#): Google has [launched](#) a series of flexible online courses focused on high growth technology to equip Australians with high-demand digital skills - including in IT Support, User Experience (UX) Design, Data Analytics, Project Management and Digital Marketing. As part of this program, we have created a consortium involving leading Australian organisations who recognise the value of these qualifications and are interested in placing graduates in jobs. This consortium includes Australia Post, Woolworths Group, Canva, Optus and IAG. We are also partnering with prominent community partners to offer 10,000 free scholarships with a focus on women and First Nations Australians.
- **Cybersecurity:** Google takes a comprehensive approach to security, which keeps millions of Australian Internet users safe online. Our approach is guided by a set of principles that we believe can help policymakers improve security;
 - We believe digital technologies should be secure by default. Security is foundational to digital trust and safety, and is at the very core of every Google product and service.
 - We develop advanced capabilities to help raise the security bar for all. That’s why in 2021 we pledged to invest \$10 billion in global cybersecurity innovation and in partnerships with industry peers, governments, and civil society groups to solve previously intractable problems.
- **Sustainability and climate change:** Google is enabling the use of AI for natural disaster detection and post-disaster rebuilding applications to strengthen Australia’s resilience against the impacts of climate change - a \$1.4 million grant from Google.org, our philanthropic arm, has allowed researchers to use AI for real-time predictions of bushfire hazards.

Our economic impact in Australia

Google is proud of the economic impact we have in Australia. Since we started with just one person in a Sydney lounge room twenty years ago, we have grown to a team of more than 2,000 people in Australia and our digital products and services are supporting millions of Australian businesses and individuals across the economy.

Through products and services including GoogleAds, AdSense, Play, Ad Grants, Search, Maps and Cloud, AlphaBeta estimates that Australian businesses gain \$47.1 billion worth of economic

value annually. Of this value, 61 per cent went to small and medium-sized Australian businesses. These products are helping businesses expand and grow revenue in domestic and international markets, and work more efficiently. Further, we estimate that this helps support an additional 133,300 jobs, with a further 186,500 jobs enabled across businesses' supply chains across the country.

Many of our products, most of which are free to use, have become an important part of the everyday lives of millions of Australians. By using Google Search, Maps, Play, Drive, Photos, Docs and Sheets, Australian consumers enjoy \$19.5 billion worth of annual benefits, representing an average of \$763 of annual value to each Australian internet user.

Separately, Oxford Economics has estimated that YouTube's creative ecosystem contributed over \$1.4 billion to Australia's GDP in 2021 and supported more than 18,000 full-time equivalent jobs in Australia in that same period.

Strong competition across the technology sector

Competition is thriving across the technology sector, involving small and large, local and global digital companies and this is providing significant benefits for small businesses and users. Companies that are not constantly innovating, improving and developing new products will fail.

Australia sits in a region where there is intense competition and users are deeply integrated into technology - Asia-Pacific is the number one region for mobile app subscription growth, averaging a 27 per cent annual increase.

The dynamic nature of competition in the technology sector is marked by the rapid growth of new players and innovations in products and services. Some examples include:

- **Search:** Today, Australians have more ways to search for information online than ever before – and increasingly this is happening outside the context of general search engines like Google Search or Microsoft's Bing. For example, when searching for products online, Australians are using services like Amazon or specialised providers in areas like travel, real estate, or local services. Furthermore, a number of AI platforms have recently emerged, embedding AI in their services. These developments create more ways for people to find content and highlight how competitive and dynamic this part of the tech industry is, to the benefit of consumers. For example, we have seen the emergence of NeevaAI, Microsoft's USD\$10 billion investment in ChatGPT maker OpenAI and AI-powered Bing search engine. Google also announced its own plans to use generative AI language models in Search.¹

¹ Google, '[An important next step on our AI journey](#)', The Keyword (6 February 2023).

- **Online advertising:** Microsoft acquired ad tech provider Xandr and signed a landmark deal to build Netflix's advertising business. Amazon's advertising business is now growing faster than Google and Meta's advertising businesses, to quickly be half the size of Amazon's Web Services (AWS) business. Apple's advertising business is expected to reach over \$30 billion in the next four years. Only five years after launching outside of mainland China, TikTok is reported to have nearly \$10 billion in advertising revenue and continues to grow rapidly.

These examples underline the extent to which digital markets can evolve quickly and unpredictably with disruptive new entrants reshaping products and services and forcing incumbent players to respond and innovate.

Innovation to the benefit of consumers and businesses

Google has over time innovated our products and services to provide richer search results for the benefit of consumers and businesses. For example, if a user searches for [hospitals open now near me], we can return a list of results that are actually hospitals, that are located near the user, that are open at the time of the query, and we identify the locations of the hospital on a map. This is much more useful for users than merely showing a list of blue links to webpages.

Our differentiation of our search results in this way helps people find what they are looking for as quickly and easily as possible and make it easy for businesses to connect with customers. This is not anti-competitive but innovation that benefits consumers. The innovation and development of new features is a sign of a healthy competitive ecosystem - increasing competition among firms for the benefit of consumers who enjoy better products and lower prices.

Australia's competition policy framework

Australia has a robust competition law framework that has been developed to address harms to competition and consumers. The *Competition and Consumer Act 2010* contains broad and flexible prohibitions on conduct and arrangements that are likely to substantially lessen competition. Quite rightly, the focus of the framework is on promoting the welfare of Australian consumers, while promoting competition, economic efficiency and innovation.

The effectiveness of this framework in the context of digital platforms is currently subject to a number of reviews, including the ACCC's [Digital Platform Services Inquiry](#) and Treasury's

[consultation on Digital Platform regulatory reforms](#). Google is actively contributing to these processes, including with insights from our interaction with regulation globally.²

International developments highlight that there is no “one size fits all” approach to competition policy for digital platforms. Jurisdictions are taking very different approaches to regulation, including:

- Regulators taking action through existing frameworks (e.g., the US Department of Justice enforcement actions)
- Legislation on specific areas of conduct (e.g., Korea regulating app stores)
- Ex ante regimes enshrined in legislation (e.g., the EU’s Digital Markets Act)
- Bespoke codes of conduct (e.g., UK Digital Markets Unit).

These various approaches are still nascent and we believe policy makers can take time to observe these developments and consider the best approach for Australia.

System transparency

Transparency is essential to Google gaining and maintaining the trust of our users and society. Digital products and services should not be black boxes – that is why Google has invested over the past few years to better explain how our systems work³.

We believe transparency measures must **be helpful and meaningful**. Users should be able to easily access information that gives them a sense not only as to what data is used and for what purposes, but also provides an understanding of how the service works, and shows what the important design characteristics behind the system are. In the context of search engines, for example, that means stating the parameters that determine things like ranking and prominence, and the relative importance of each parameter.

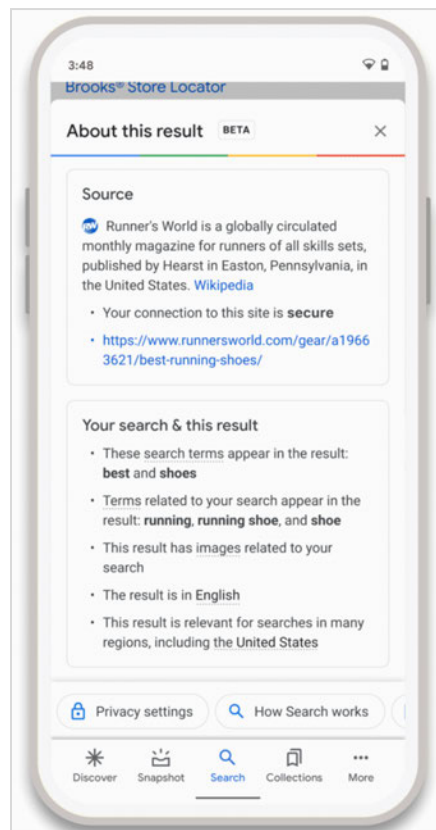
We believe Google strikes the right balance in its approach to these important questions. Our product policies and public blogs provide detailed overviews and timely information on Google’s approach to explaining how our most important systems work for billions of people every day. We offer public and easily-digested resources available to everyone that outline the guiding principles, design factors, and signals that our systems use in the real world. For example, we recently published our [Guide to Google Search Ranking Systems](#) on [Google Search Central](#), and anyone can visit our websites that describe in detail [How Search Works](#), [How news works on Google](#), or [How YouTube Works](#) to learn not only about how our systems operate but also about the robust processes Google has in place to ensure adherence to those

² See: [Google submission to ACCC App Stores inquiry](#) (March 2021) / [Google submission to ACCC web browser and general search services inquiry](#) (September 2021) / [Google submission to ACCC regulatory reform inquiry](#), [Supplementary Submission 1](#), [Supplementary Submission 2](#) (September 2022)

³ See: [How ‘Google Search Works’](#)

principles. We also offer researchers affiliated with accredited higher education institutions access to YouTube’s global Data API through our [YouTube Researcher Program](#).

We are also continuing to invest to purposefully build digital literacy and transparency-enhancing features directly into our products to provide users with easy ways to understand and evaluate the results they are seeing. For example, on Google Search our [About This Result](#) panel empowers users to see more context about any Search result before they ever visit a web page, just by tapping the three dots next to the result and has been used billions of times by users. We are currently working to add more content to the About this Result panel to provide all Australian users with a quick and easy way to see useful context about how Google returned results for a specific query. This feature will include showing searchers information about the most important ranking factors used by Google Search to connect results to their queries. These factors help Google to determine when results may be relevant and providing real time transparency to users will help Australians develop greater search literacy and decide what result may be useful to them. Some of the factors users may see include matching keywords, related terms, looking at links, and local relevance. We are working to bring this functionality to Australia in the coming months.



Example of Google’s “About This Result” panel in Search

We also empower users by giving them significant control over personalised recommendations. On YouTube, for instance, users can control what data is used to

personalise recommendations by deleting or pausing activity history. Clearing watch history means that a user will not be recommended videos based on content they previously viewed. Users can also clear their search history, remove individual search entries from search suggestions, or pause search history using the YouTube History settings, and set parameters to automatically delete activity data in specified time intervals, and stop saving activity data entirely.

When it comes to calls specifically for system transparency and the desire to ensure algorithms are accountable, we agree that these are important guiding principles for governing the use of algorithms in our society, and it is equally important that society has confidence in the techniques used to achieve them. . The approach taken by digital service providers to provide transparency and accountability should be risk-based, proportional, technically and operationally feasible, and include robust protections for intellectual property and user privacy among others.

Any approach to setting expectations about system transparency must be balanced and account for both the potential benefits and real world risks involved, and allow the flexibility to tailor by context. This starts with system operators taking into account what level of transparency is actually operationally and technically feasible, useful to users, and will enable accountability. For example, each year for Google Search we make more than 5,150 improvements to our systems after conducting over 800,000 experiments which are evaluated by 16,000 independent search raters. When operating at this scale it is neither practical nor desirable to talk about transparency at the level of line-by-line code changes. Advanced notification processes not only detract from our ability to design the best products for Australian users, but they also risk significantly slowing down rates of innovation. Rather, it is important to explain the guiding principles, factors, and signals that determine how our algorithms operate in the real world. That is why Google's process for making system changes is available for anyone to read via our [detailed and publicly available guidelines](#).

It is often assumed that transparency – simply making more information publicly available or subject to disclosure – will lead to greater accountability and trust. But it is critical in this discussion to acknowledge the many important trade-offs that need to be carefully balanced to protect the privacy and security of Australian users. Any approach must include strong protections for intellectual property and take steps to protect trade secrets and commercially sensitive information to avoid enabling bad actors that seek to manipulate or game digital systems for their own illegitimate purposes. Sharing source code or detailed advanced descriptions of system architecture changes, model weights and parameters can further enable malicious actors to game AI systems (for example, evading classifiers that identify malicious content), enable cyberattacks, expose users' private data, or infringe on intellectual property rights.

Google has learned the hard way that unbounded transparency is not in anyone's best interests⁴ – there are reasons we need to block over 40 billion spam sites per day. Protecting the integrity of our systems against interference by state and non-state actors is a big part of what drives us to continuously invest to improve and to protect the millions of legitimate Australian businesses and users that trust and use our systems. This is why efforts to provide system transparency must be risk-based and proportional.

Data and privacy

Privacy is at the heart of everything we do at Google. With one of the world's most advanced security infrastructures, our products are **secure by default**. We strictly uphold responsible data practices so every product we build is **private by design**. And we create easy to use privacy and security settings so users are **in control**. We never sell users' personal information to anyone.

We also invest in research and development of leading privacy and security engineering techniques, and share what we learn to benefit the broader ecosystem. We set the standard then keep improving our approach to privacy innovation.

We even challenge the assumption that products need more personal information to be helpful. For example, we invented federated learning, a new approach to machine learning that enables Google's products to work better without collecting raw data from a device. Federated learning is how Google's Keyboard can recognise and suggest new words after thousands of people begin typing them without Google seeing what is written. We're also deploying differential privacy, which enables us to provide useful features – like showing how busy a place is over the course of a day in Maps – while mathematically guaranteeing an individual's data cannot be distinguished or re-identified.

We recognise that people want more control over their presence and experiences online and we have developed the following easy to use tools that put control back in the hands of Australians.

- **Google Account.** You can find key information, privacy, and security settings all in your Google Account. We have created easy-to-use tools like Dashboard and My Activity, which give you transparency over data collected from your activity across Google services. There are also controls like Activity Controls and Ad Settings, which allow you

⁴ Even simply providing some details of the elements that go into the algorithm can lead to harmful results. In 1999, Google's founders published a seminal paper on a key innovation in Google's algorithm: PageRank. This algorithm analyses the links between pages to assess the importance of websites. We learned that publishing this inspired spammers to game Google by [paying each other](#) for links, harming both legitimate businesses and consumers who sought accurate information.

to switch the collection and use of data on or off to decide how all of Google can work better for you.

- **Privacy Checkup.** Each year, over 100 million Google customers take a Privacy Checkup to understand what information is being shared and easily make changes to their settings. In just a few minutes, you can choose what types of data are saved to your Google Account, update what you share with friends or make public, and adjust the types of ads you would like us to show you.
- **Auto-delete controls.** Auto-delete settings let you choose a time limit for how long you want to keep your Location History, YouTube, and activity data. Data older than the limit you choose (3 or 18 months) will be continuously and automatically deleted from your account.
- **MyActivity.** My Activity is the central place where you can find everything you've searched, viewed, and watched using our services. To make it easier to recall your past online activity, we give you tools to search by topic, date, and product. You can permanently delete specific activities or even entire topics that you don't want associated with your account.
- **Google Assistant.** Answers like "Hey Google, how do you keep my data safe" and delete Assistant activity from your Google Account just by saying things like "Hey Google, delete the last thing I said to you".
- **Incognito mode.** When you turn on Incognito mode in Maps, Chrome and YouTube, your activity, like the places you search for, websites you've visited or the videos you watch, won't be saved to your Google Account. Browsing history and cookies from your Incognito session are deleted from Chrome once you close all Incognito windows.
- **My Ad Centre.** We recently launched more controls for ads privacy settings: a way of choosing which brands to see more or less of, and an easier way to choose whether to personalise ads. My Ad Centre gives even more control over the ads you see on YouTube, Search, and your Discover feed, while still being able to block and report ads. You'll be able to choose the types of ads you want to see — such as fitness, vacation rentals or skincare — and learn more about the information we use to show them to you.
- **YouTube.** As mentioned above, as a user, you can control what data is used to personalise recommendations by deleting or pausing activity history. As a creator, you can choose to keep your content private or public. For our younger users, YouTube has additional privacy controls to prioritise their safety and well-being. For example, we have set the default upload setting to the most private option available for users aged 13-17. Younger users who would like to make their content public can change the default upload visibility setting. YouTube also limits personal data collection from visitors on YouTube sites made for younger users (e.g., YouTube Kids and Supervised Experiences).

- **Results in Search:** When you're using the internet, it's important to have control over how your personal information can be found. With our new tool to accompany updated removal policies, people can more easily request the removal of Google Search results containing their contact details — such as phone numbers, home addresses, and email addresses.

We aim to continually learn and improve our privacy program and the transparency, control, and security that we build into our products. With tools like Download Your Data and Chrome Incognito mode, we are at the forefront of how to apply privacy controls and protections into service offerings and data governance. We have practical experience building systems that apply our privacy principles, which helps us meet legal compliance obligations in Australia and around the world.

Role of regulation

We support robust, economy wide and evidence based privacy regulation but we're not waiting on new regulations to improve on our privacy program, and the safeguards, transparency and controls we build into our products. Google published a [framework for data protection legislation](#) in 2018 based in part on Google's practical experience developing products and services that make use of personal data, and from our experience with Australian and international data protection frameworks. We are deeply engaged in the current review of Australia's Privacy Act. We believe that, at its core, comprehensive federal legislation should be risk - and outcomes - based, consistent, adaptable, and work for all types and sizes of businesses and organisations. Legislation should focus on responsible and reasonable data collection and use; transparency; control; security; access, correction, portability, and deletion; adaptability; and accountability. It should apply to all businesses and organisations that process personal information, and all data that can be used to identify an individual.

Children's safety

At Google, we believe that technology can be a force for good - unlocking creativity, fostering expression, and learning skills that help children and young people build their futures. At the same time, we recognise that technology can also be used to cause harm to people and to children in particular, with the potential to facilitate abuse and exploitation.

We work to help protect children while also enabling them to play, express themselves and learn online. This includes:

- Building innovative products – to be used to protect children and to be used by children and their families to provide them with age-appropriate experiences and protections and help families develop the balance that works for them;
- Putting in place extensive policies that enable us to respond to new and evolving trends, developing industry-leading tools that help us detect abusive content at scale; and
- Working with experts and creating a program of global education that helps children with digital literacy and digital citizenship to help them better navigate life online.

Google is one of the [industry leaders](#) in fighting child sexual abuse and exploitation online. We invest heavily in fighting it and use our proprietary technology to deter, detect, remove and report offences on our platforms. We partner with NGOs and industry on programs to share our technical expertise, and develop and share tools to help organisations fight Child Sexual Abuse Material (CSAM). We also work with law enforcement worldwide to report CSAM instances quickly and thoroughly. Our goal is to prevent offenders from using our services to share and distribute this material.

We approach this fight against CSAM by 1) developing and sharing technology to **detect** this content at scale; 2) **reporting** child sexual abuse material on our platforms (see [transparency report](#)); 3) **detering** predatory behaviours on our platforms that put children at risk; and 4) **working across industry and with NGOs** to support the development of new data-driven tools, boost technical capacity, and raise awareness.

Responsibility is our number one priority across all Google products and we've invested in a number of technologies and efforts⁵ to protect young people when they use various Google products, including;

- Family Link
 - In 2017, Google launched Family Link; an app where parents can create a Google account for their under 13 year old child, and directly supervise aspects of their child's account and their device activity.
 - The app allows parents to set certain digital ground rules -- like helping to manage the apps their child can download, setting screen time limits, setting a bedtime for the child's device and turning on location sharing (so that the supervising parent can see the location of the device).

⁵ See: <https://blog.youtube/news-and-events/an-update-on-our-efforts-to-protect?m=1>

- YouTube

- We launched the standalone [YouTube Kids app](#) (2015) for users under the age of consent and a [supervised experience on the main YouTube app](#) (in 2021) for pre-teens and older.
- In 2021, we changed the default upload setting to the most private option available for teens ages 13-17.
- We provide safeguards and education about commercial content for minors, and surface a variety of digital wellbeing features. This includes turning on 'take a break' and bedtime reminders by default and turning off autoplay for users under 18.
- We empower YouTube content creators with tools to determine who should see their content. Not only can they use [privacy settings](#) to share videos with just friends and family or small groups, but we also require them to [age-restrict their own content](#) when appropriate. When content is age-restricted, users coming to YouTube must be signed-in with a Google account and their account age must be 18 or older in order to view the video. If they aren't signed in or their account age is under 18, they see a warning and are redirected to find other content that is age-appropriate. Additionally, if our systems are unable to establish that a viewer is above the age of 18, we will request that they provide a valid ID or credit card to verify their age. Our [Community Guidelines](#) include [guidance](#) to uploaders about when content should be age-restricted. YouTube's Trust & Safety team also applies age-restrictions when, in the course of reviewing content, they discover a video that isn't appropriate for viewers under 18 and has not already been put behind an age restriction.
- We partnered with experts, such as Professor Amanda Third of Western Sydney University, through our [Youth and Families Advisory Committee](#) to develop a set of [quality principles](#) to guide creators making kids and family content. These best practices are intended to support child development and wellbeing by promoting things like being a good person through modelling respect or healthy habits, learning and curiosity, play and imagination and diversity. Our systems also promote content in line with these principles.

- Search

- We have a range of systems, tools, and policies that are designed to help people discover content from across the web while not surprising them with mature content they haven't searched for. One of the protections we offer is [SafeSearch](#), which helps filter out explicit results when enabled and is turned on by default for all signed-in users under 13 and make this the default setting for teens setting up new accounts.

- Google removes images of anyone below the age of 18 from search results at the request of the individual under 18 or their parent or guardian, with the exception of cases of compelling public interest or newsworthiness⁶.
- Location History
 - Location History is turned off by default for all accounts, and is disabled for children under the age of 18 (with no option to turn it on).
- Advertising
 - We prevent age-sensitive ad categories (e.g. diet and weight loss, gambling, alcohol) from being shown to teens, and we block ad targeting based on the age, gender, or interests of people under 18.
- Privacy
 - We have developed new resources to help children and teens better understand our privacy practices including a Teen Privacy Guide that helps teens better understand key questions about data practices on our platforms. While our Privacy Policy already includes audiovisual resources and snippets with definitions of key terms that facilitate comprehension by teens, the new Teen Privacy Guide is an additional resource in a Q&A format that our research shows resonates better with teens and uses language that is even more tailored to their age.
 - We have also created a [Family Link Privacy Guide](#) to explain key aspects about the processing of data by Google and the supervision tools available to parents as part of Family Link. We are creating several versions of this resource; each of them tailored to a different age band to enhance comprehension.
 - We will begin introducing bite-sized notices in Search and YouTube to children and teens explaining key concepts in main products.

Last year, we also expanded our age assurance policy for YouTube and Google Play to Australia. This added step is informed by the Australian Online Safety (Restricted Access Systems) Declaration, which requires platforms to take reasonable steps to confirm users are adults to access content that is potentially inappropriate for viewers under 18.

As part of this process some Australian users may be asked to provide additional proof of age when attempting to watch mature content on YouTube or downloading content on Google Play. If our systems are unable to establish that a viewer is above the age of 18, we will request that they provide a valid ID or credit card to verify their age. We've built our age-verification process in keeping with Google's [Privacy and Security Principles](#).

As part of our efforts in this important area, we have engaged extensively with the several recent and ongoing initiatives led by the government and its agencies. This has included

⁶ See further detail: '[Remove images of minors from Google Search results](#)'

significant involvement and input to inform the dialogue on age assurance and restricted access. With the consolidation of the online safety legislation into the new Online Safety Act in 2021, we've been working through the past year to detail its implementation in the form of eight parallel codes each tailored to distinct sectors of the online environment, focusing on illegal content - particularly child safety issues.

As this new Code is being finalised and the broader Online Safety Act is being implemented, our focus is to make this new framework and the Basic Online Safety Expectations, effective in practice, together with our longstanding initiatives to fight these abuses through means such as technological developments and supporting initiatives such as online safety awareness raising. Now that we have such an extensive body of law, it is incumbent upon all of us, from government agencies to digital platforms and others such as specialist civil society groups and support services, to work together to make it work on the ground through concrete and earnest actions.

Mis / Disinformation

Google continues to believe that the Internet is a boon to society – contributing among others to global education, healthcare, research, and economic development by enabling citizens to become more knowledgeable and involved through access to information at an unprecedented scale. However, like other communication channels, the open Internet is vulnerable to the propagation of false or misleading information.

These concerns directly affect Google and our mission – to organise the world's information and make it universally accessible and useful. When our services are used to propagate deceptive or misleading information, our mission is undermined. How companies like Google address these concerns has an impact on society and on the trust users place in our services. We take this responsibility very seriously and believe it begins with providing transparency into our policies, inviting feedback, enabling users, and collaborating with policymakers, civil society, and academics around the world.

We have an important responsibility to our users and to the societies in which we operate to curb the efforts of those who aim to propagate false information on our platforms. At the same time, we respect our users' fundamental human rights (such as free expression) and we try to be clear and predictable in our efforts, letting users and content creators decide for themselves whether we are operating fairly. Of course, this is a delicate balance, as sharing too much of the granular details of how our algorithms and processes work would make it easier for bad actors to exploit them (as mentioned above in the section concerning transparency).

Our approach to tackling mis/disinformation in our products and services is based around a framework of three strategies: make quality count in our ranking systems, counteract malicious actors, and give users more context.

Mis/disinformation is a complex challenge, and in the absence of a silver bullet to deal with this issue, there is a lot of value in ways to make society as a whole more resilient to these harms, and that a range of relevant stakeholders have roles and responsibilities for: alongside digital platforms, other actors such as government of course, as well as civil society, researchers, journalists and the news media, and fact checking communities.

Media literacy is an obvious, but important starting point. By investing in training for school-age children and for adults as well, governments can make it more likely that citizens will think twice before believing or resharing a piece of mis/disinformation content. In 2020, Google invested \$1.4m in the development of the [Media Literacy Lab](#) to ensure that young Australians aged 12-16 are being taught critical thinking skills and basic fact checking techniques. We've also formed [a partnership](#) with [Squiz Kids](#) - Australia's premier daily news podcast made just for kids - to launch Newshounds in Australian and New Zealand schools. It's a plug-and-play media literacy teaching resource for children between 8 and 12 years, comprising podcasts and accompanying in-classroom activities, helping children, their parents and teachers to decide if they should believe what's in front of them

Similarly, supporting the work of journalists and fact-checkers is a fundamental component of ensuring that citizens have access to information that they trust and that has the potential to steer them away from disinformation. Funding, training, or dedicated programs for journalists should be part of the whole-of-society response.

Google and YouTube are firmly engaged in both of these efforts – we support media literacy campaigns all around the world, via our own programs (such as YouTube's [Hit Pause](#), a global media literacy campaign developed in partnership with the National Association for Media Literacy to teach viewers to become better critical thinkers and more digitally responsible) and by funding third party efforts with Google NewsLab and Google.org. In addition, our Google News Initiative supports newsrooms all around the world to help them reach new audiences online, better leverage technology for their work, and evolve business models so as to find more paths to profitability.

Governments are right to want to ensure that key stakeholders such as platforms are taking disinformation seriously.

However, in this fast-moving field, regulatory approaches that optimise for flexibility and leave ample room for experimentation are the best way forward. They enable progress in the short term while avoiding the risk of enshrining into law responses or frameworks that might prove counterproductive or outdated in the months that follow.

Governments should instead ensure that each relevant platform has an action plan that addresses the specifics of disinformation as it manifests on its services; that this plan is communicated clearly and that regular reports are shared on progress; and that these plans are reevaluated at regular intervals so as to iterate upon them as needed.

Commitments or best practices or formal Codes of Practice can be effective instruments to strike that balance, and so we welcome the approach taken by Australia with the initiative started in 2021 with the Code of Practice on Mis/disinformation. We are confident that it sets out the right commitments and practices to foster an effective and durable impact on the problem as it affects Australian Internet users. We were one of the first companies to sign on to this code and have published annual compliance reports⁷ outlining how we are meeting the commitments contained within the code.

While we sometimes hear calls for regulation of mis/disinformation, no regulation is without trade-offs, and as the Inquiry Issues paper underscores, it is not necessarily the case that it is always needed.

For a start, regulation should be careful to avoid harming legitimate expression and other unintended consequences—some of which may be counterproductive, especially in an area as nuanced and challenging as misinformation.

As rightly noted by the Inquiry, undermining legitimate speech is a major concern: as legal definitions in this field are new and emerging, it will be very challenging to design legislation that does not end up inadvertently including expression that the government would wish to remain legal. In addition, any unclear regulation on speech may have chilling effects – leading people to self-censor as they are not sure about what is legal and what is not. In the worst case scenario, as the Inquiry rightly points out, going as far as *de facto* establishing a regulatory or government body that would be empowered to act as a ‘ministry of truth’ to correct or remove false content online is very likely to be counterproductive, and could prove devastating for the right to free speech.

We note that the threat models continue to evolve as bad actors change their attack patterns and Internet uses change over time—remedies that were effective two years ago may not be best suited to the next wave of challenges.

Relatedly, adding a regulatory layer to the existing framework would risk making it impossible for platforms to adapt: we have learned from watching bad actors over the past years that they are quick to adapt to new boundaries set by platforms. For example, in response to increased scrutiny on foreign interference, some have started hiring local proxies to publish content on their behalf. Inflexible laws risk setting in stone a specific defence that would soon prove obsolete, and that companies would be powerless to change.

A legislative approach could also mandate interventions that have unanticipated and counterproductive consequences: because we know relatively so little about what is effective to tackle disinformation and it is constantly evolving, it is always possible that an intervention that seems safe and helpful today might be proven to be counterproductive tomorrow.

⁷ See: <https://digi.org.au/disinformation-code/transparency/>

The cloud

Besides consumer services, Google also provides cloud services to enterprise customers. Google Cloud's mission is to accelerate every organisation's ability to digitally transform and reimagine their business through data-powered innovation. The following section lays out our perspective of the provision of cloud services in Australia.

Importance of cloud services to Australian businesses

Cloud is the key enabler to facilitate Australian companies' digital transformation and significantly reduce their IT spend, which in turn leads to greater innovation, choice and competition. The global pandemic further accelerated digital adoption, and the cloud industry has contributed significantly to Australian businesses' ability to rapidly shift online and scale their presence. Further context on the importance of cloud services more generally is [here](#).

Competitive landscape in cloud services

Google Cloud's infrastructure business officially launched in 2012 as a competitor to well-established players like Amazon Web Services (AWS) and legacy hard- and software vendors like Microsoft, IBM and Oracle. Beyond the two largest providers of cloud infrastructure services, AWS and Microsoft Azure, is a dynamic and fragmented set of smaller competitors including a number of multinational providers (such as Google Cloud, Alibaba, IBM Kyndryl, Oracle, VMWare and Cloudera).

The International Data Corporation (IDC) estimates that AWS (40%) and Microsoft (22%) are the two clear leaders in cloud services by global revenue share.⁸ Other players with substantially lower shares include Google (5.5%), Alibaba Group (6.1%) and IBM (2.5%). In Australia, AWS and Microsoft have a leading position.

Importance of interoperability, openness and portability in cloud services

It is important that the cloud market works well for Australian government customers, businesses and end-consumers while ensuring a fair playing field across all layers of the value

⁸ IDC, Worldwide Public Cloud Services, 2021. Based on Foundational Cloud Services, which IDC defines as the Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service – System Infrastructure Software (SaaS – SIS) segments. See: IDC, '[Worldwide Public Cloud Services Revenues Grew 29.0% to \\$408.6 Billion in 2021. According to IDC](#)' (29 June 2022)

chain. From the outset, Google Cloud has been a strong advocate of facilitating multicloud and customer choice⁹.

Unlike the closed proprietary systems of traditional IT players, Google Cloud's services are based on open source technologies that are designed to be compatible and interoperable with other cloud services. This reduces technical barriers, enhances users' ability to multicloud with other cloud providers and helps address many sovereignty requirements by reducing technical dependencies on a single vendor. Google entered the market having developed its cloud services directly in the cloud without building on pre-existing positions in 'on-premise' or legacy IT products. Google and others have been successful in growing their businesses by responding to customer dissatisfaction with traditional IT service providers and supporting 'multicloud' options, i.e. supporting customer use of more than one cloud provider.

It is worth noting in more detail why the tenets of interoperability, openness and portability are critical to customer choice and competition in the cloud market:

- a. Interoperability, which is the ability of systems to work efficiently and collaborate effectively across different cloud platforms, drives down the costs of multi-homing and intensifies competition between cloud providers who must compete for new and existing business based on the quality and costs of their services.
- b. Portability allows a customer to move and suitably adapt their applications and data between: their own systems and cloud services, cloud services of different providers and potentially different cloud deployment models.¹⁰ An important aspect of this is data portability, which Google believes is key to mitigating potential future risks posed by market concentration, and mitigating against the potential harms caused by technical and contractual lock-in.
- c. Open Source: Many modern cloud platforms, including Google's, originated from open source software.¹¹ Open source and open source-based technologies (such as containers, open APIs, and open source databases) are enablers of multicloud and often go hand-in-hand with increasing customer choice, as they support movement of workloads and data across different cloud environments¹².

⁹ For more detail on ensuring fair and open competition in cloud, see: Blog: '[Ensuring fair and open competition in the cloud](#)'

¹⁰ [Interoperability and Portability for Cloud Computing: A Guide Version 2.0 \(omg.org\)](#)

¹¹ As discussed above, open source is a foundation of Google's strategy. This started 15 years ago with process containers and has since developed into 9000 active open source projects that Google continues to maintain. See also [IDC White Paper: Modernize Applications with Open Source Software on Google Cloud](#).

¹² See: [IDC White Paper: 'How a Multicloud Strategy can help Regulated Organizations Mitigate Risks in Cloud'](#) (March 2021)

As outlined above, Google is proud to be the first to launch a multicloud infrastructure service (allowing customers to manage workloads across multiple clouds) and the first to launch a multicloud data warehouse (allowing customers to analyse data across multiple clouds). Google Cloud has a long history of sharing technology through open source—from projects like [Kubernetes](#), which is now the industry standard in container portability and interoperability in the cloud (as discussed below), to [TensorFlow](#), a free and open source software library for machine learning and artificial intelligence. Adoption of these open source technologies enables customers to easily move their applications to or from Google to other cloud providers that support such environments. This is a key differentiator of Google Cloud and lies at the heart of Google’s customer-centric proposition.

It is also standard industry practice for cloud providers to offer portfolios of services, including in partnership with independent software vendors and other cloud providers (i.e. including those that compete with their own offerings), which allow them to better serve their respective customers. Such open “ecosystems” are highly beneficial to independent software vendors (and ultimately their end-customers) by providing them with an additional marketing and distribution channel, more payment security and facilitating ease of software deployment on public cloud infrastructures.

The benefits of a competitive cloud industry based on interoperability, portability and open source solutions cannot be overstated.¹³ The industry itself is taking steps to further foster best practices across markets, including self-regulatory initiatives such as SWIPO Data Portability CoC and the EU Cloud CoC, CISPE’s [Fair Software Principles](#) and the [Coalition for Fair Software Licensing](#) which aim to develop an open cloud universe that promotes the interests of all cloud users. Google fully supports such initiatives and continues to advocate for widespread industry adoption. However, ultimately, these initiatives can only achieve their envisaged customer benefits if all industry players are willing to play by the same principles of fairness and openness.

Importance of ensuring competition in cloud services

Google firmly believes that the benefits of cloud are maximised when customers are free to choose from the full range of cloud solutions that best suit their needs. The benefits of cloud are reinforced by strong competition across all layers of cloud services, allowing customers to choose from a wide array of services, product propositions and payment models that best suits their needs. Widespread adoption of multicloud strategies and switching practices have enhanced competition in this space, which has seen cloud providers competing vigorously to develop new technologies and solutions to meet evolving customer needs / use cases.

Cloud is at an inflection point in the contest between legacy software constructs—restrictive licensing, closed ecosystems and tying—and the cloud’s original promise and potential—open,

¹³ See: [Google submission](#) to Ofcom Cloud services market study

elastic and free from artificial lock-ins. While interoperability and open source technologies are prevalent across the industry (including in response to increasing demand from customers who seek to deploy a multicloud approach), a small number of cloud providers (in particular, some legacy on-premise IT providers) nevertheless seek to give their own cloud products an unearned advantage and lock customers into their cloud ecosystems. At this critical moment when migration to the cloud is progressing at pace, unfair licensing restrictions on cloud services could have harmful impacts resulting in less user-choice, higher costs, lower quality, reduced security and stunted innovation.

Importantly, restrictive contracting and tendering practices are often not transparent to industry participants in confidential tender processes, and cloud customers may not appreciate the disadvantages of restrictive terms until they later seek to add new cloud functionality or switch some services (or consider upfront price too attractive to refuse in any event). With overly complex agreements that lock in clients for years to come, some legacy software vendors may be forcing customers toward a monolithic cloud model, but also creating downstream effects that would limit choice and potentially disrupt growing and thriving digital ecosystems around the world.

Regulatory oversight of cloud services

There are a number of laws, regulations and policy frameworks in Australia that provide oversight of cloud services. Depending on whether a cloud provider services government or commercial customers (or both), the cloud service provider may be subject to a number of direct or indirect oversight regimes, including (but not limited to):

- [Hosting Certification Framework](#)
- [Infosec Registered Assessors Program](#)
- CPS231 and CPS234- APRA Outsourcing Guidance
- CPS230 (effective 1 January 2024)
- Security of Critical Infrastructure Act 2018
- Privacy Act 1988
- Competition and Consumer Act 2010

A key objective of any regulatory or compliance oversight should be to harmonise, streamline and de-duplicate the regulatory frameworks applicable to the sector the subject of regulation. We consider that the existing frameworks and obligations provide sufficient oversight of cloud service providers in the Australian market, without the need to introduce further regulation or compliance obligations.

However, Google recommends a greater emphasis on examining restrictive licensing, tying and other practices that can negatively affect competitive outcomes in cloud, as noted above.

Data security and privacy in the cloud

Security and privacy can be optimised when cloud-based services are free to leverage distributed network infrastructure without geographic restrictions. We can offer customers robust security solutions across globally distributed infrastructure, or we can provide enterprise-grade security, while ensuring data remains within geographic boundaries.

Availability, disaster recovery, and business continuity are an essential part of running a business or providing government services in today's digital economy. Unfortunately, earthquakes, hurricanes, floods, and other natural or human-made disasters are also an inevitable occurrence. Organisations will not survive if they do not have the ability to withstand and quickly recover from such events. Leveraging a globally distributed network like Google Cloud, which intelligently distributes data and applications through a geographically diverse network, enables businesses to confidently backup critical data and quickly recover and respond when disaster strikes. Laws, regulations or policies that require an organisation's data or applications to remain in one physical location dramatically increase the likelihood that a single catastrophic event will be insurmountable.¹⁴

We recognise we need to meet our customers on the journey where they are - that's why we have launched [digital sovereignty offerings in Australia](#) to give customers controls and other capabilities that help them achieve their desired level of digital sovereignty, meet regulatory obligations while maximising the benefits of modern cloud solutions when it comes to feature availability, reliability, scalability and cost.

Utilisation of cloud services across borders

Alignment with international standards ensures best practices are utilised, promotes interoperability, and avoids introducing unnecessary and burdensome complexity. This avoids conflicting standards and reduces complexity for customers of technology services and for companies providing products or services to the Australian market. Importantly, it would also help Australian companies seeking to enter export markets to minimise development costs. Further information on this is contained in [Google's submission](#) to the data security strategy consultation process.

Google welcomes the opportunity to provide the above information to the Committee in support of its inquiry.

¹⁴ For further information, see Google's white paper on [Digital Sovereignty in the Cloud](#), and additional information on [Google customer controls and open cloud solutions](#).