Computer & Communications Industry Association

Tech Advocacy Since 1972

CCIA's Comments to the ACCC Digital Platforms Inquiry Preliminary Report

February 15, 2019

Computer & Communications Industry Association
Tech Advocacy Since 1972

Table of Contents

Executive Summary of CCIA Responses to ACCC Recommendations i

1. Introduction 1

2. Market Power & Digital Platforms 2
- **2.1 The Term "Platform"** 2
- **2.2 Network Effects** 3
- **2.3 Data as a Dimension of Competition** 4
- **2.4 Accumulation of Data Does Not Protect a Company from Competition** 5
- **2.5 Algorithmic Decision Making** 7
- **2.6 CCIA's Response to the ACCC's Recommendations 1-3** 8

3. Digital Advertising 11
- **3.1 Competition in Advertising** 11
- **3.2 CCIA's Response to the ACCC's Recommendations 4-6** 12

4. Digital Content 14
- **4.1 Intermediary Liability Safe Harbors** 14
- **4.2 CCIA's response to the ACCC's Recommendation 7** 14

5. Privacy 15
- **5.1 Interoperability** 16
- **5.2 Algorithmic Fairness** 16
- **5.3 CCIA's response to the ACCC's Recommendations 8-11** 18

Computer & Communications Industry Association
Tech Advocacy Since 1972

Executive Summary of CCIA Responses to ACCC Recommendations

1. Merger Law: The ACCC's proposed recommendation to explicitly include the effects on potential competitors as part of the merger control test, and to single out the role of data in transactions is futile.

2. Prior Notice of Acquisitions: The ACCC proposes to impose additional commitments from 'large digital platforms', and therefore to move away from an industry-agnostic competition system. The implementation of the second recommendation will reduce legal certainty and distort the level playing field.

3. Choice of Browser and Search Engine: The ACCC recommends to impose a prohibition on suppliers of operating systems for mobile devices, computers, and tablets as well as a prohibition on suppliers of internet browsers to offer default browser and default search engines. This type of recommendation resembles industrial-policy interventions that limit the benefits achieved through business negotiation and leveraging that leads to lower prices and a better consumer experience. Instead, CCIA believes that the correct approach to potential tying and bundling issues is an evidence-based framework which focuses on actual harm to the consumer, and not on penalizing a firm merely because it is dominant.

4-6. Advertising & Related Business Oversight; News and Digital Platform Regulatory Oversight & Review of Media Regulatory Frameworks: Rather than fracture enforcers' jurisdiction and create expensive, duplicative regulatory structures aimed at businesses that have drawn the ire of prominent news publishers, CCIA proposes that (a) competition and consumer protection enforcers receive adequate resources to address their mandate and that (b) issues related to digital platforms (however defined) be addressed by existing consumer protection authorities using their existing statutory tools. In addition, the idea to create an algorithmic regulator as suggested in Recommendation 4 in pursuit of transparency about search ranking parameters, would compel disclosure of trade secrets.

7. Takedown Standard: The ACCC suggests that the ACMA determine a mandatory standard regarding digital platforms' takedown procedures for copyright infringing content. CCIA urges Australia to instead come into compliance with its long-unmet commitments made to the United States in the 2003 Australian United States Free Trade Agreement (AUSFTA).

8(a). Notification Requirements: The ACCC recommends the introduction of an express requirement that the collection of personal information be accompanied by a notification that is concise, transparent, intelligible and easily accessible. CCIA supports effective notice, but cautions against the development of overly prescriptive notification requirements.

8(b). Independent Third-Party Certification Scheme: CCIA opposes regulations containing requirements that arbitrarily target certain organizations. The ACCC's proposal to develop an "objective threshold" for mandating that organizations undergo external audits by OAIC is futile.

8(c). Increasing Consent Requirements: The ACCC proposes amendments to designate consent under the APPs as express and opt-in consent; however, this will create an overly complex and confusing experience for consumers. Alternatively, the ACCC suggests prohibiting entities from collecting, using, or disclosing personal information of Australians for targeted advertising purposes unless consumers have provided express, opt-in consent. CCIA opposes this suggestion, as it is likely to harm the digital economy with no clear benefit.

8(d). Erasure of Personal Information: The ACCC recommends enabling a consumer to require the erasure of their personal information where they have withdrawn consent and the personal information is no longer necessary to provide the consumer with a service. CCIA supports enabling consumers to request the erasure of personal information where practicable and provided that deletion does not implicate the personal information of others. The ACCC also invites views on the feasibility of an obligation to delete all user data when a user leaves a service or after a set period of time. This suggestion is both infeasible and harmful to socially beneficial research and innovation.

8(e). Increasing Penalties: The ACCC suggests increasing the penalties for breaches of the Privacy Act to mirror the recently increased penalties for breaches of the Australian Consumer Law. Any expansion of civil penalties for privacy violations must be linked to clear principles of enforcement and be supported by economic analysis to ensure that potentially beneficial innovation is not stymied.

8(f). Introducing Direct Rights of Action for Individuals: The ACCC recommends giving individual consumers a direct right to bring actions for breaches of the Privacy Act. CCIA believes that enforcement should be tailored to actual harm or risk of harm and that a private right of action would be unduly burdensome on organizations and divert business resources away from socially beneficial activities.

8(g). Expanding Enforcement Resources: The ACCC recommends providing increased resources to equip the OAIC to deal with increasing volume, significance, and complexity of

privacy-related complaints. Additionally the ACCC suggests that it may be appropriate to grant OAIC additional legislative powers to improve its ability to enforce the Privacy Act, such as the power to require publication of notifiable data breaches and steps taken to minimize the risks of harm. CCIA supports appropriate allocation of resources and authority to enable regulatory agencies to fulfill their missions.

9. OAIC Code of Practice for Digital Platforms: The ACCC proposes to recommend that the OAIC to engage with 'key' digital platforms to develop an enforceable code of practice containing specific obligations on how digital platforms must inform consumers and how to obtain consumers' informed consent, as well as appropriate consumer controls over digital platforms' data practices. In CCIA's view it is inappropriate and futile to attempt to identify 'key' digital platforms in this manner.

10. Serious Invasions of Privacy: The ACCC proposes to recommend that the Government adopt the ALRC's recommendation to introduce a statutory cause of action. In CCIA's view, a private right of action is inappropriate as it would not meaningfully empower ordinary consumers, but would create substantial uncertainty for organizations.

11. Unfair Contract Terms: The ACCC proposes to recommendation that unfair contract terms should be illegal (not just voidable) under the ACL, and that civil pecuniary penalties should apply to their use. In CCIA's view, this would create significant uncertainty for organizations, chilling socially beneficial innovation and data uses.

Computer & Communications Industry Association
Tech Advocacy Since 1972

1. Introduction

The Computer and Communications Industry Association (CCIA)[1] welcomes the opportunity to submit comments to the Preliminary Report that the Australian Competition and Consumers Commission (ACCC) released on the 4th of December, as a result of its inquiry into digital platforms (the Preliminary Report).

CCIA agrees with the ACCC that the so-called digital platforms offer innovative and popular services to consumers, and have revolutionized the way consumers and businesses interact with each other. However, CCIA believes that the preliminary report does not fully reflect the nature of the multi-sided business models, and therefore has mischaracterized the market dynamics in which many of the businesses mentioned in the Preliminary Report operate. The Preliminary Report fails to identify concrete areas where consumers are being harmed, and includes recommendations that are clearly disconnected from any potential consumer harm.

CCIA believes that for the ACCC and regulators and competition authorities across the world to determine whether there is a need to address possible concerns from consumer protection and competition viewpoints, it is important to fully and accurately understand the business models behind the so-called "platforms", as well as the advertising markets. In fact, the ACCC's Preliminary Report suggests, among others, creating a new authority aimed at regulating algorithms which will certainly diminish consumers' welfare and their ability to make informed decisions about what they want to see online. Most importantly, it will be very detrimental to the progress of innovation.

When conducting this type of inquiry, CCIA encourages authorities to take into account real-world business realities and ensure that incumbents do not influence the real competitive dynamics behind the markets, as such a position would go against consumers' benefits. As such, it is important that the ACCC reexamine its Preliminary Report to fully reflect the underlying business models of these complex services and revisit its preliminary recommendations accordingly.

[1] CCIA represents large, medium and small companies in the high technology products and services sectors, including computer hardware and software, electronic commerce, telecommunications and Internet products and services. Our members employ more than 750,000 workers and generate annual revenues in excess of $540 billion. A list of CCIA members is available at https://www.ccianet.org/members.

2. Market Power & Digital Platforms

2.1 The Term "Platform"

The term "platform" is frequently used in reference to certain Internet-related business models, but usually without any definitional rigor. In lieu of these terms, the concept of "two-sided" or "multi-sided" markets is better substituted for "platforms" when considering competition policy matters.[2] Multi-sided business models are not new and have existed for centuries. However, they have more recently proliferated across the economy, providing for a variety of customers to realize immediate benefits due to the ability of these business models to readily facilitate interactions among multiple parties. As discussed below, multi-sided business models have grown in recent years as a variety of Internet services have utilized the business model of pairing providers of goods, services, or content with consumers of those goods, services, or content, thanks to the power of the Internet to bring people together regardless of geography. Their success has generated vibrant debate on how antitrust enforcement should address these types of enterprises.

When enforcing antitrust laws with respect to multi-sided business models, agencies should also take into account the diverse nature of business models that exist, as is done when analyzing single-sided markets. Predatory pricing is a good example of how failure to account for the interdependent demand that characterizes multi-sided business models can lead agencies to police false positives, by concluding that conduct is anti-competitive when, in fact, it is not. If a multi-sided business is charging a below-cost price on one side, and antitrust enforcement authorities fail to account for the other relevant sides of the business at issue, authorities would reach an inaccurate conclusion regarding the business's conduct. Pricing below cost is a common profit-maximizing behavior of multi-sided business models because of potential differences in elasticity of demand on different sides of the business, even when operating in competitive industries, and should not be considered actionable, anti-competitive conduct without additional truly probative evidence.[3]

---

[2] Daniel O'Connor & Matthew Schruers, *Against Platform Regulation*, Presentation Draft, Oxford Internet Institute Conference on Internet, Policy, and Politics (Oct. 2016) at 3-8, *available at* http://blogs.oii.ox.ac.uk/ipp-conference/sites/ipp/files/documents/OConnor-Schruers%2520-%2520Against%2520Platform%2520Regulation.pdf.

[3] *See id.*; David S. Evans, *The Antitrust Economics of Multi-Sided Platform Markets*, 20 YALE J. ON REG. 325, 343 (2003); David S. Evans & Michael Noel, *Defining Antitrust Markets When Firms Operate Two-Sided Platforms*, 2005 COLUM. BUS. L. REV. 667, 681-82 (2005).

2.2 Network Effects

Network effects, or demand side economies of scale, are present when the value of adopting a service to an incremental user is larger when more users have already adopted that service.[4] The evaluation of network effects in competition analyses should be accompanied by analysis concerning the extent to which "single-homing" and "multi-homing" are present in a given market.[5]

For example, Professors Haucap and Heimeshoff acknowledge that:

> In two-sided markets increasing concentration will be driven by indirect network effects, but capacity limits, product differentiation and the potential for multi-homing (i.e., the parallel usage of different platforms) will decrease concentration levels. How easy it is for consumers to multi-home depends, among other things, on (a) switching costs (if they exist) between platforms and (b) whether usage-based tariffs or positive flat rates are charged on the platform.[6]
>
> "Multi-homing" refers to those instances where customers use more than one platform or service, whereas "single-homing" refers to those instances where customers only use one platform or service in a particular industry. Compared to previous physical networks, many of today's online platforms may be more susceptible to disruption from new entrants thanks to lower barriers to entry, low switching costs, the prevalence of free-to-the-user business models, and multi-homing.

As argued by economist David Evans:

> Online platforms are more susceptible to attack by entrants than network industries of a century ago. Network effects and sunk costs made the natural monopolies around the turn of 20th century difficult to challenge. Rivals had to sink massive amounts of capital into duplicating physical networks such as railroad tracks and telephone lines. Using multiple networks, or switching between them, was expensive for customers, even if a second network was available. However, online platforms can leverage the Internet to provide wired and wireless connections globally. People find it generally easy, and often costless,

[4] *See, e.g.* Hal R. Varian, *Use and Abuse of Network Effects* (Sept. 17, 2017), *available at* https://ssrn.com/abstract=3215488.

[5] *See* Jean-Charles Rochet & Jean Tirole, *Two Sided Markets: A Progress Report*, 37 RAND J. ECON 646 (2006); Jean-Charles Rochet & Jean Tirole, *Platform Competition in Two-Sided Markets*, 1 J. EUR. ECON. ASS'N 990 (2003).

[6] Justus Haucap & Ulrich Heimeshoff, *Google, Facebook, Amazon, EBay: Is The Internet Driving Competition Or Market Monopolization?*, Düsseldorf Institute for Competition Economics (Jan. 2013).

> to use multiple online platforms, and many often do. The ease and prevalence of multihoming have enabled new firms, as well as cross-platform entrants, to attract significant numbers of users and secure critical mass necessary for growth. Incumbent platforms then face serious competitive pressure from new entrants—startups or other online platforms—because their network effects are reversible.[7]

In sum, the presence of network effects, as well as other competitive constraints such as multi-homing, merit analysis when analyzing antitrust laws on multi-sided business models. Generalizations may be difficult, and a case-by-case analysis that takes into account evidence, economic analysis, and that is specific to the facts remains key to safeguarding consumer welfare.

2.3 Data as a Dimension of Competition

Intervention in data-driven markets without evidence of harm to competition could harm consumers and deter innovation, especially when based on a misunderstanding or incorrect understanding of the role data plays in these markets. Therefore, understanding the nature of data usage in Internet and technology services is crucial.

Data itself should not be seen as a barrier to entry, or to automatically grant a competitive advantage in the market. Data is characterized by the so-called "Four Vs", namely:

> **Volume**: The amount of data available, which is infinite and non-rivalrous.
> **Velocity**: The speed of data generation, which requires business to update datasets quickly.
> **Variety**: The diverse forms of data that are available to companies.
> **Veracity**: The trustworthiness of data.[8]

The mere accumulation of data, in and of itself, is useless and not of importance to compete effectively. In addition to the Four Vs, data must be analyzed before it becomes useful. As such, the value of data only appears once companies have processed such data. As economists Anja Lambrecht and Catherine Tucker note:

---

[7] David Evans, *Why The Dynamics Of Competition For Online Platforms Leads To Sleepless Nights, But Not Sleepy Monopolies* (2017), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3009438.

[8] *See* IBM, The Four V's of Big Data - Infographic, *available at* http://www.ibmbigdatahub.com/infographic/four-vs-big-data (last visited July 20, 2018).

> Our analysis suggests that big data is not inimitable or rare, that substitutes exist, and that by itself big data is unlikely to be valuable. There are many alternative sources of data available to firms, reflecting the extent to which customers leave multiple digital footprints on the internet. In order to extract value from big data, firms need to have the right managerial toolkit. The history of the digital economy offers many examples, like Airbnb, Uber and Tinder, where a simple insight into customer needs allowed entry into markets where incumbents already had access to big data. Therefore, to build sustainable competitive advantage in the new data-rich environment, rather than simply amassing big data, firms need to focus on developing both the tools and organizational competence to allow them to use big data to provide value to consumers in previously impossible ways.[9]

The authors further conclude that the tools used to analyze the data and 'provide value to consumers' confer a 'sustainable advantage' to companies rather than the mere possession of data.[10]

2.4 Accumulation of Data Does Not Protect a Company from Competition

The key to gaining a competitive edge in the digital economy is not the accumulation of data, but rather, the capacity to analyze and monetize data. In other words, human capacity and better products such as improved algorithms, rather than data or scarcity thereof, is what is necessary to compete in data-driven markets.

Stanford University conducted a study to analyze whether increased accumulation of data improved the outcomes of the analysis performed on such data. The Stanford Dogs Dataset contains images of 120 breeds of dogs from around the world.[11] This dataset was constructed for the purpose of fine-grained image categorization. Researchers used this dataset for classifying breeds of dogs in images, and calculated the mean accuracy for identification as the number of images in the dataset increased. The results showed that additional access to data provided diminishing returns to the accuracy of classification results (see chart below).[12] In short, a growing dataset provided diminishing returns as it grew.

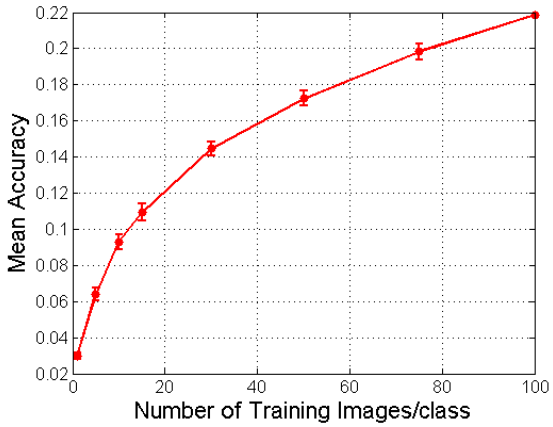
---

[9] Anja Lambrecht & Catherine Tucker, *Can Big Data Protect a Firm from Competition* (Dec. 18, 2015), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2705530.

[10] *Id.*

[11] Stanford Dogs Dataset, *available at* http://vision.stanford.edu/aditya86/ImageNetDogs/.

[12] *Id.*



Similarly, economists David Evans and Richard Schmalensee found that across technology companies, data did not grant incumbents the power to strangle competition. Their research highlighted that:

> A number of previously dominant companies all had user data — so-called "attention platforms" such as AOL, Friendster, Myspace, Orkut, Yahoo!, Blackberry in mobile, as well as numerous search engines including AltaVista, Infoseek, and Lycos. This data did not give the incumbents the power to stifle competition in their respective markets, nor is there any evidence that data increased the network effects for these firms in a way that gave them a substantial lead over challengers.[13]

Professor Daniel Sokol and Central University of Finance and Economics School of Law (China) Professor Jingyuan (Mary) Ma conclude that little, if any, user data is required as a starting point for most online services. They noted that:

> The data requirements of new competitors are far more modest and qualitatively different than those of more established markets. Little, if any, user data is required as a starting point for most online services. Instead, firms may enter with innovative new products that skillfully address customer needs, and quickly collect data from users, which can then be used towards further product improvement and success.[14]

This research shows why the accumulation of data alone is not a tool for companies to shut out competitors, and is unlikely to lead to decreased competition in the relevant market.

---

[13] David S. Evans & Richard Schmalensee, *Network Effects: March to the Evidence, Not to the Slogans*, Antitrust Chronicle (Aug. 2017) at 9, *available at* http://mitsloan.mit.edu/shared/ods/documents/?DocumentID=4243.

[14] D. Daniel Sokol & Jingyuan (Mary) Ma, *Understanding Online Markets and Antitrust Analysis*, 15 NW. J. TECH. & INTELL. PROP. 43 (2017), *available at* https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1267&context=njtip.

2.5 Algorithmic Decision Making

Firms' use of algorithms to set prices should be generally seen as an efficient way to increase market competition to the benefit of consumers. It is regular practice for firms to monitor competitors' prices and adapt accordingly in order to compete. Therefore, the use of price algorithms injects dynamism in the markets as it allows firms to adapt price setting rules more rapidly. There is no special characteristic of firms' usage of price algorithms to compete that elicits changes to the current competition framework. Nothing about the use of algorithms confers immunity from antitrust law. As illustrated, price algorithms are mostly pro-competitive. In the limited instances where firms could use algorithms to the detriment of consumer welfare, these actions can be addressed using current antitrust enforcement tools.

Algorithms and Price Discrimination

Price discrimination and dynamic pricing, or the capacity to change and adapt prices in view of evolving estimates of the supply and demand relationship for a particular product, is pro-competitive. Pricing algorithms allow firms to engage in price discrimination and dynamic pricing in a more efficient manner to respond more quickly to changes in the market, increasing price competition. Additionally, the use of algorithms can help firms to allocate resources more efficiently. Allocative efficiencies bring generally positive outcomes that benefit consumer welfare. Finally, firms can use competitors' pricing as an input to optimize their own pricing algorithm and offer more competitive prices to customers, again increasing market competition to the benefit of consumers.

Algorithms and Collusion

While the use of algorithms based on competitors' data is generally considered pro-competitive, concerns have been voiced that the increased price transparency online can enable tacit collusion and/or help firms to engage in illegal agreements.

Firms may use algorithms to monitor agreed-upon prices, engage in explicit collusion, or to implement pre-existing explicit collusion. Current U.S. antitrust laws would apply to such agreements, and the use of such algorithms for collusive purposes would form evidence of an illegal agreement among competitors. Agreement by competitors to coordinate their own pricing algorithms is no different than human-created cartels, and thus redressable where appropriate under the current antitrust regime. The more science-fiction variation of collusion, in which autonomous pricing algorithms engage in explicit collusion with each other, remains beyond any

real world scenario. Regulating collusive agreements formed without human interaction is implausible, and collusive agreements formed through human agency are fully prohibited by existing law.

There have been discussions concerning how algorithms can facilitate tacit collusion, *i.e.*, "conscious parallelism," that may result in a lessening of price competition. In the United States, tacit collusion remains legal under the current antitrust framework. As clearly expressed in U.S. case law, and recognized by U.S. antitrust agencies themselves, "[w]ithout proof of collusion or evidence that the knowing parallel adoption of pricing formulas narrowed the range of prices over time, parallel pricing conduct may be outside the reach of the antitrust laws."[15]

Tacit collusion *facilitated* by algorithms would still require certain market and economic conditions to exist (such as market transparency, deterrent mechanisms, absence of competitors' or customers' reaction, or a punishing mechanism for colluders). Given the difficulty to encounter market conditions that would allow tacit collusion to exist, and that the alternative would be to regulate prices, the antitrust approach to tacit collusion should remain intact, even if firms expand their use of pricing algorithms.

Finally, price algorithms may also be used by firms in a pro-competitive manner by engaging in aggressive competition. Firms could use pricing algorithms to undercut rivals, and to engage in disruptive pricing strategies; the aggressive competition as a result would benefit consumers.

2.6 CCIA's Response to the ACCC's Recommendations 1-3

CCIA's Response to the ACCC's Recommendation 1: Merger Law

The ACCC's proposed recommendation to explicitly include the effects on potential competitors as part of the merger control test, and to single out the role of data in transactions is futile.

To ensure that tech-related innovation continues to play a positive role in the economy, sound competition policy and antitrust enforcement must both play a crucial role in ensuring that

[15] Algorithms and Collusion - Note by the United States, Submission to OECD Competition Committee (May 26, 2017), *available at* https://one.oecd.org/document/DAF/COMP/WD(2017)41/en/pdf.

competition exists across markets. Merger control, as part of the antitrust toolkit, remains a key element in ensuring that the economy remains dynamic. Merger control laws are aimed at reviewing the potential anticompetitive effects of transactions and allowing competition authorities to analyze the anticompetitive effects of transactions, including effects on the competitive landscape. In this respect, the effects on market entry of competitors or potential competitors are already taken into account, when engaging in the analyses to determine the potential anticompetitive effects of a transaction.

As such, it would be against the consumer welfare standard to amend the merger control rules to allow the ACCC to engage in an artificial effort to try to guess what 'potential competitors' could be beyond the established test, as it wouldn't be based on credible evidence. Having an authority guess what the potential competitors would be in a given market would give a role to the ACCC distant from maintaining competition in the markets, and closer to acting as an organizer of the industries at stake.

Furthermore, the ACCC proposal to make it even more clear that in the context of a merger data has to be analyzed as an important asset would not have any impact on the activities of the competition authority. Data, as any other asset, is already being taken into account when reviewing transactions, and therefore what the ACCC recommends is already part of the existing toolkit.

For all these reasons, CCIA believes that the ACCC should continue to enforce merger control rules and evaluate transactions based on sound economic analysis that focuses on real and potential harm to consumer welfare. Given the growing politicization of transatlantic antitrust enforcement, it is crucial for the ACCC to continue to advocate for an evidence-based enforcement approach.

CCIA's Response to the ACCC's Recommendation 2: Prior Notice of Acquisitions

The ACCC proposes to impose additional commitments from 'large digital platforms', and therefore to move away from an industry-agnostic competition system. The implementation of the second recommendation will reduce legal certainty and distort the level playing field.

One of the common features of existing competition authorities worldwide is that they tend to be industry-agnostic. This is the main reason why competition norms are considered to be dynamic, adaptable to all industries, and have survived over decades. The ACCC proposal to request commitments from large digital platforms risks destroying the stability of the competition system, promoting negative effects on consumers due to, *e.g.,* increased legal uncertainty.

First, the concept of large digital platforms is vague. The preliminary report refers specifically to Facebook and Google, which is strongly indicative that the rule targets specific American Internet companies. Second, the classification of companies as 'large digital platforms' is so unclear that it will likely open the door for political interference and regulatory capture. Third, the adoption of such a rule will certainly create mistrust in competition norms by allowing companies to take advantage of such a vague norm and of the competition system as a means to avoid competing on the merits. All of these factors combined will lead the ACCC to engage in arbitrary decisions, and will eventually distort the level playing field against the benefit of consumers.

CCIA's Response to the ACCC's Recommendation 3: Choice of Browser and Search Engine

The ACCC proposes to impose a prohibition on suppliers of operating systems for mobile devices, computers, and tablets as well as a prohibition on suppliers of internet browsers to offer default browser and default search engines. This type of recommendation resembles industrial-policy interventions that limit the benefits achieved through business negotiation and leveraging that leads to lower prices and a better consumer experience. Instead, CCIA believes that the correct approach to potential tying and bundling issues is an evidence-based framework which focuses on actual harm to the consumer, and not on penalizing a firm merely because it is dominant.

For a competition authority to consider the recommendation of a measure that would limit the benefits of having a market economy and adopt a posture more aligned with industrial organization is extremely worrisome. Competition policy has progressively moved towards ensuring, on a case-by-case basis, that recommendations are based on evidence and enhance consumer welfare.

As a matter of example, the European Commission has considered the pre-installation of a company's product in a variety of services and suppliers in the past. In 2011, the European Commission found during the Microsoft/Skype merger review process that the vast majority of

consumers who acquired a PC with Skype already installed were registered Skype users and that most of them subsequently downloaded a version different from the pre-installed one.[16] The European Commission also found that these possible barriers to entry were not considered significant by respondents to the market investigation. On the contrary, consumers can download the software of an alternative provider easily and for free.

CCIA therefore rejects ACCC's solution to impose a prohibition on suppliers of operating systems for mobile devices, computers and tablets as well as a prohibition on suppliers of internet browsers to offer default browser and default search engines.

3. Digital Advertising

3.1 Competition in Advertising

The ACCC raises concerns about the market power of Facebook and Google in digital advertising, when in fact, advertising remains a highly competitive marketplace where on-line and off-line channels compete fiercely. Furthermore, players in digital advertising remain in direct competition for ad dollars spent on radio, TV, outdoor & cinema, and print media. See Appendix A for an infographic explaining how ad dollars are spent in the advertising marketplace.[17]

Over the past 20 years the internet economy has disrupted traditional advertising models, bringing benefits to both advertisers and consumers. However, competition for consumer attention, and in turn, advertising revenue, remains fierce between mediums. Furthermore, new technologies and innovation will continue to disrupt the advertising marketplace. For example, television advertising will increasingly take advantage of new tools such as granular set-top box data to personalize ads to the viewer.

Even within the digital advertising market, platforms like Google and Facebook compete with a variety of services for user attention, all of which have the opportunity to display relevant advertising. This includes services such as messaging, gaming, streaming, various search engines, social media, and video, both on desktop and mobile, with new arrivals appearing

[16] Case No COMP/M.6281 - Microsoft/Skype, Regulation (EC) No 139/2004 Merger Procedure, Office for the Publication of the European Union (July 10, 2011), *available at* http://ec.europa.eu/competition/mergers/cases/decisions/m6281_924_2.pdf

[17] Matt Schruers, *Infographic: How Ad Dollars Are Spent*, Disruptive Competition Project, Jan. 16, 2018, *available at* http://www.project-disco.org/competition/011618-how-ad-dollars-are-spent/#.XGSMm_x7kck

regularly. Major media, telecom, and Internet competitors have expanding advertising revenue or are planning significant investments into the digital advertising market.[18] Furthermore, the ACCC's estimation that Google and Facebook have captured 80% of all growth in digital advertising over the past three years fails to recognize that the majority of the revenue for ad placement is passed on to the sites where the ads are placed. For example, Google transfers 68% of advertising revenue for content with publishers.[19]

3.2 CCIA's Response to the ACCC's Recommendations 4-6

CCIA's Response to the ACCC's Recommendations 4-6: Advertising & Related Business Oversight; News and Digital Platform Regulatory Oversight & Review of Media Regulatory Frameworks

Rather than fracture enforcers' jurisdiction and create expensive, duplicative regulatory structures aimed at businesses that have drawn the ire of prominent news publishers, CCIA proposes that (a) competition and consumer protection enforcers receive adequate resources to address their mandate and that (b) issues related to digital platforms (however defined) be addressed by existing consumer protection authorities using their existing statutory tools.

In addition, the idea to create an algorithmic regulator as suggested in Recommendation 4 in pursuit of transparency about search ranking parameters, would compel disclosure of trade secrets.

The preliminary report proposes the creation of a *sui generis* regulatory entity with antitrust and competition enforcement responsibilities, focused solely on the narrow industry segment of "digital platforms," specifically those platforms that "rank news and journalistic content." As noted above in Section 2.1, "platform" is as an amorphous term, which policymakers have long struggled to define meaningfully. Wrestling with this, the preliminary report points to "search engines, social media platforms and digital content aggregation platforms" before simply naming the intended targets, Google and Facebook. The report never proposes a working definition that could potentially include Australian firms.

[18] Mark MacCarthy, *Competition in Digital Advertising is On the Rise*, CIO (Dec. 19, 2018), accessible at https://www.cio.com/article/3328650/amazon-com/competition-in-digital-advertising-is-on-the-rise.html.

[19] Google, AdSense Help, *available at* https://support.google.com/adsense/answer/180195?hl=en.

By recommending this new *sui generis* regulator be empowered to take action again "discriminatory conduct…not limited to… anticompetitive conduct", the proposed report appears to contemplate regulators prohibiting *pro*-competitive conduct that benefits consumers but displeases news publishers. Vertical integration is a practice that increases efficiency and enhances competition, and the ACCC should not penalize it. A broad mandate to treat business users' competing goods and services "equally" would be un-administrable even if a special algorithm regulator is created, and would create uncertainty and confusion. The proposal to prohibit a handful of firms from discriminating among competitors in a *pro-competitive* fashion is a radical one.

It is particularly problematic that such an authority would be empowered to second-guess the "criteria" used by online platforms in opining on the relative relevant of journalistic publications to a particular user's inquiry. These opinions, although data-driven, are ultimately a subjective view on what users are likely to find most relevant to their interests. No doubt, every content producer would like to be first in any ranking of content producers. It would be highly inappropriate, however, to insert government views into this process. No regulator should prescribe the criteria an online service may use in formulating its own opinions on content relevance to its users.

This is not to suggest that all recommendations by online services are immune from regulatory scrutiny. If an online service were to represent that its services employ one metric (such as proposed relevance) in making recommendations, but in fact used another (*e.g.*, paid placement), the failure to disclose that would likely constitute an unfair business practice. As the U.S. FTC indicated to search engines in 2013, failing to "clearly and prominently distinguish[] advertising from natural search results" could run afoul of U.S. consumer protection law, specifically Section 5 of the FTC Act.[20] In fact, such a "garden-variety" misrepresentation falls well within the scope of traditional consumer protection enforcement, and is in not unique to the Internet environment. Accordingly, a new regulatory with Internet-specific jurisdiction is unnecessary and duplicative.

[20] U.S. Federal Trade Comm'n, *FTC Staff to Search Engines: Differentiate Ads from Natural Results*, June 25, 2013, https://www.ftc.gov/news-events/blogs/business-blog/2013/06/ftc-staff-search-engines-differentiate-ads-natural-results

4. Digital Content

4.1 Intermediary Liability Safe Harbors

The need for harmonization of critical intermediary liability protections, also known as safe harbors, in Australian copyright law, is an important issue in the digital economy.

AUSFTA contains an obligation to provide liability limitations for service providers, analogous to 17 U.S.C. § 512 in the U.S. However, Australia has failed to fully implement such obligations and current implementations are far narrower than what is required under AUSFTA. Australia's statute limits protection to what it refers to as "carriage" service providers, not service providers generally. The consequence of this limitation is that intermediary protection is largely limited to Australia's domestic broadband providers.

4.2 CCIA's response to the ACCC's Recommendation 7

CCIA's response to the ACCC's Recommendation 7: Takedown Standard

The ACCC suggests that the ACMA determine a mandatory standard regarding digital platforms' takedown procedures for copyright infringing content. CCIA urges Australia to instead come into compliance with its long-unmet commitments made to the United States in the 2003 Australia-United States Free Trade Agreement (AUSFTA).

Article 17.11.29 of AUSFTA requires the parties to introduce limitations on the liability of providers of Internet services for copyright infringement. The safe harbors in Article 17.11.29 address four separate Internet functions or activities identified. Those distinct activities are: (1) transmission, routing, or providing connections ("mere conduit"); (2) automatic caching; (3) storage ("hosting"); and (4) referring or linking to an online location.

AUSFTA requires that these four safe harbors extend to "service providers." Article 29(b)(xii) provides two different meanings for two different types of "service provider." For the mere conduit functions, "service provider" means "a provider of transmission, routing, or connections for digital online communications without modification of their content between or among points

specified by the user of the material of the user's choosing." For the functions of caching, storage, and referring or linking users to an online location, "service provider" more generally means "a provider or operator of facilities for online services or network access."

However, the Australian implementation of this safe harbor obligation, codified at sections 116AA et seq. of the Copyright Act 1968, applies only to "carriage service providers" rather than "service providers." Sections 7 and 87 of the Telecommunications Act 1997 define a "carriage service provider" as a provider to the public of a service for carrying communications by means of guided and/or unguided electromagnetic energy. In essence, the existing scheme provides safe harbors only to part of one of the two categories of service providers required by AUSFTA — providers of mere conduit services to the public. The definition of carriage service provider excludes both (1) providers of conduit services to a limited universe of users (*e.g.*, a college's students); and (2) providers of facilities for online services that do not also provide conduit services to the public (*e.g.*, a search engine or a web host).

The Australian government has recognized this inconsistency in multiple proceedings[21] with some proposals properly expanding the safe harbors to include the necessary functions.[22] Unfortunately, these proposals were tabled. Amending the Copyright Act to extend safe harbors to all service providers is essential in order for Australia to comply with its obligations under AUSFTA. The current disparity harms competition and innovation for Internet services in Australia, especially startups and small businesses — including domestic companies.

5. Privacy

The sustainability and continued growth of the digital economy requires that consumers trust companies to protect their personal information. Beyond that, organizations have a duty to respect individuals' interests when they process personal information. Therefore, CCIA supports privacy principles that ensure that data is handled responsibly and transparently, and that allow consumers to exercise reasonable control over their personal information. To promote predictability and drive a healthy data ecosystem, privacy regulations should be technology neutral, meaning they should not provide specific technology mandates; sector-neutral, meaning they should apply to online and offline companies; and should provide for safe harbors and flexibility for companies to make adjustments according to the needs of consumers.

[21] Australian Attorney-General's Department, Consultation Paper: Revising the Scope of the Copyright Safe Harbour Scheme (2011), https://www.ag.gov.au/Consultations/Documents/Revising+the+Scope+of+the+Copyright+Safe+Harbour+Scheme.pdf; Australian Government Productivity Commission, Intellectual Property Arrangements Recommendations (Sept. 2016), http://www.pc.gov.au/inquiries/completed/intellectual-property/report/intellectual-property-overview.pdf.

[22] Copyright Amendment (Disability Access and Other Measures) Bill 2016.

Privacy regulations must be designed to ensure that consumers can continue to benefit from innovation and new technologies. Restricting companies' use and collection of data may unintentionally impair digital commerce and reduce investment. Therefore, privacy regulations should focus on preventing measurable consumer harms while affording room for innovation.

5.1 Interoperability

Competition between digital services based on their privacy and security attributes can help consumers choose services that best align with their personal privacy preferences. Scholars Ramon Casadesus-Masanell and Andres Hervas-Drane demonstrated that in the marketplace for services partly dependent on information disclosure for revenue (used as a proxy for how protective of privacy a service might be), competition can drive the provision of services with more privacy protective features. However, where the net utility of a service far outweighs the value consumers place on data protection, that service will continue to outperform competitors who are offering an ostensibly more privacy protective service.[23] This research indicates that consumers seek to optimize various features, including privacy, in maximizing their own personal utility without the need to have a special regulator patronizing consumers.

Casadesus-Masanell and Hervas-Drane point to principles that can help ensure that these risks related to enhancing operability bring about are mitigated and consumers are empowered. In particular, these authors suggest that to ensure data transfers between systems are private, secure, and balanced, data portability tools should be voluntary, industry-developed, and responsive to actual consumer needs.[24]

5.2 Algorithmic Fairness

With respect to privacy and data protection, algorithmic and AI-enabled decision-making systems pose similar risks to other data-intensive technologies. Several academics, building on the work of Daniel Solove, have identified the privacy risks in the algorithmic space, including: exclusion in information processing, a lack of data subject disclosure and control in processing,

[23] Ramon Casadesus-Masanell & Andres Hervas-Drane, Harvard Business School, Working Paper (2013), *available at* https://www.hbs.edu/faculty/Publication%20Files/13-085_95c71478-a439-4c00-b1dd-f9d963b99c34.pdf.

[24] For example, they should: (1) allow users to move data they have provided to the service, but not data that may relate to other users; (2) afford consumers control over how and when the tools are used; and (3) be tailored to the privacy and security expectations of specific products and services.

and reputational distortion.[25] Some automated decision-making systems may also pose the risk of inadvertent disclosure of an individual's personal information or protected status.[26]

These privacy risks can generally be mitigated through traditional privacy- and security-by-design methods of product and service development. Businesses should ensure that privacy risks are considered in the collection and use of data. This means that data used for automated decision-making processes, namely those powered by machine learning algorithms, is: (1) lawfully collected and used; (2) securely stored; and (3) representative of the population that these decisions will be applied to. Businesses should: (1) detect and mitigate biases in their systems before rolling out their products; (2) invest in and apply—whenever possible—sound measures to de-identify the data used to train algorithmic model; and (3) provide users with control over and meaningful transparency about algorithmic decision-making processes.

The increased use of algorithms and AI-enabled tools for decision-making in business, social, and political contexts has raised concerns that algorithms or their decisions might exhibit or exacerbate human bias or discrimination. The complexity of algorithmic and machine learning-based decision-making tools suggests that in some cases it may be difficult for designers or external reviewers to determine the procedural basis for their outputs, even when those decisions or predictions tend to be more reliable and accurate than their human-derived counterparts. Further, the speed and scale at which such systems may make decisions means that they could amplify potential disparate impacts. Researchers have identified three scenarios where bias might be reflected in a decision-making system or its outputs: (1) training on implicitly biased or statistically distorted datasets; (2) potentially biased algorithm or model design; and (3) masking of intentional discrimination through the complexity of decision-making systems.[27]

Reducing the risk of bias in complex algorithmic decision-making systems requires a multi-pronged approach. Appropriate hiring practices to build diverse and cross-disciplinary teams with technical and social science expertise, combined with robust methodologies in identifying and correcting potential sources or proxies for bias in datasets or model design, can help mitigate bias before it can enter a system. Algorithmic accountability, or the idea that the potential for consumer harms can be "assessed, controlled, and redressed"[28] in an algorithmic system, is a principle that can aid businesses in ensuring systems operate in accordance with their designed

[25] Joshua A. Kroll, Joanna Huey, Solon Barocas, *et al*., *Accountable Algorithms*, 165 U. PA. L. REV. 633 (2017), *available at* https://scholarship.law.upenn.edu/penn_law_review/vol165/iss3/3/.

[26] *Id*.

[27] *Id*.

[28] World Wide Web Foundation, Algorithmic Accountability (July 2017), *available at* http://webfoundation.org/docs/2017/07/Algorithms_Report_WF.pdf at 16.

intentions and can identify and address actual harmful outcomes.[29] Operators should work to define the substantive algorithmic harms that might result from a particular system based on its likely inputs and overall design. Verifying that algorithms produce results consistent with their operators' intentions, rather than those defined harms, can be accomplished through a variety of means. For instance, system architects can implement technical parameters for consistent and procedurally regular system design, provide confidence measures associated with outputs, and conduct disparate impact assessments of results to identify and rectify potential harms before and during system use.

5.3 CCIA's response to the ACCC's Recommendations 8-11

CCIA's response to the ACCC's Recommendation 8(a): Notification Requirements

The ACCC recommends the introduction of an express requirement that the collection of personal information be accompanied by a notification that is concise, transparent, intelligible and easily accessible. CCIA supports effective notice, but cautions against the development of overly prescriptive notification requirements.

Organizations should be transparent about the types of personal information that they are collecting, why they are collecting it, and how they are using it. Furthermore, organizations should be clear about whether personal information may be transferred to third parties, how long information may be retained, and what choices and controls individuals have with respect to their personal information. In order to ensure that these disclosures are effective, privacy notices should be clear, concise, accessible, easy to understand, and always provided free of charge. However, in order to avoid notice overload and consumer fatigue, affirmative notice should not be required every time information is collected or shared with a third party if the nature of that action is fully described in the original notice and the organization's privacy policy.

CCIA cautions against the development of overly prescriptive notification requirements. Many organizations are currently exploring innovative approaches for fully informing individuals about their data collection, use, and disclosure, and for making that information relevant and actionable. In addition to consumer-testing privacy notices, some organizations are updating privacy policies with informational videos, others are making privacy controls immediately

[29] Joshua New & Daniel Castro, *How Policymakers Can Foster Algorithmic Accountability*, Center for Data Innovation (2018), *available at* http://www2.datainnovation.org/2018-algorithmic-accountability.pdf.

accessible within their privacy policy. Enacting specific obligations and processes for providing notice could restrict the development of modern and effective best practices for providing relevant and actionable notice. Instead, regulators should focus on establishing a flexible, outcome-oriented approach to promoting transparency and effective privacy notices.

CCIA's response to the ACCC's Recommendation 8(b): Independent Third-Party Certification Scheme

CCIA opposes regulations containing requirements that arbitrarily target certain organizations. The ACCC's proposal to develop an "objective threshold" for mandating that organizations undergo external audits by OAIC is futile.

In order to promote consistent, sustainable, and predictable protection of consumers' personal information, any consumer privacy-focused regulatory approach should be both technology and sector neutral and apply to all organizations that process personal information. The magnitude of harm or risk of harm to a consumer that results from a breach or misuse of data is not dependent on the size or scope of the organization processing that information. Therefore, there can be no "objective threshold" for singling out particular organizations for mandatory third-party auditing based on the size of an organization or amount of information collected.

All organizations that collect and process personal information should regularly assess the privacy risks associated with their data practices and their compliance with applicable privacy and security regulations. Lawmakers can promote accountability by setting baseline requirements, enabling flexibility for meeting those requirements, and promoting industry accountability programs and safe harbors.

CCIA's response to the ACCC's Recommendation 8(c): Increasing Consent Requirements

The ACCC proposes amendments to designate consent under the APPs as express and opt-in consent; however, this will create an overly complex and confusing experience for consumers.

Alternatively, the ACCC suggests prohibiting entities from collecting, using, or disclosing personal information of Australians for targeted advertising purposes unless consumers

have provided express, opt-in consent. CCIA opposes this suggestion, as it is likely to harm the digital economy with no clear benefit.

Organizations should provide appropriate mechanisms for individuals to exercise reasonable control over the collection and use of their personal information. However, receiving express, opt-in consent should not be mandatory for every aspect of data processing. Doing so would create an overly complex and confusing experience for consumers and undercut the ACCC's goal of promoting consumer understanding of business data practices. Additionally, responsible processing of personal information is frequently necessary to simply operate some services. Therefore, any requirements to obtain express, opt-in consent should be limited to specific circumstances involving the processing of particularly sensitive personal information.

The ACCC considers applying an express, opt-in consent requirement for participating in targeted advertising. In order to appropriately protect consumer rights and interests, privacy regulations should be carefully calibrated and proportionate to evidence-based risk of harm to consumers. While the ACCC report cites surveys of consumer opinion, it does not provide a theory of the harm or costs of targeted advertising practices. In fact, many small businesses and consumers mutually benefit from sharing and receiving relevant advertisements. Furthermore, current advertising models allow digital platforms to offer free services widely enjoyed by consumers. Requiring opt-in consent for targeted advertising is a burden that would shrink marketplaces, harm consumers, and is not outweighed by any clear benefits.

CCIA's response to the ACCC's Recommendation 8(d): Erasure of Personal Information

The ACCC recommends enabling a consumer to require the erasure of their personal information where they have withdrawn consent and the personal information is no longer necessary to provide the consumer with a service. CCIA supports enabling consumers to request the erasure of personal information where practicable and provided that deletion does not implicate the personal information of others.

The ACCC also invites views on the feasibility of an obligation to delete all user data when a user leaves a service or after a set period of time. This suggestion is both infeasible and harmful to socially beneficial research and innovation.

The ability to request erasure of personal information is an important tool for promoting consumer control in their relationship with digital platforms. Organizations should comply with consumer requests to delete personal information that has been provided to that organization when it would be practical to do so, the erasure does not implicate the personal information of others, and the information is no longer necessary for the purposes for which it was initially collected. Critically, however, the concept of "erasure" should not be extended to include a so-called "right to be forgotten" (the compelled de-listing of public information) which has negative impacts on free speech rights.

In addition to an obligation to comply with reasonable erasure requests, the ACCC should consider issuing recommendations strengthening the complimentary rights of: (1) access to one's own personal information held by an organization (under APP 12); (2) the ability to correct, amend, or complete personal information (under APP 13); and (3) the right to download and move data an individual has provided to an organization in a machine-readable format with appropriate safeguards (data portability). These are effective tools for promoting consumer knowledge of data holdings and practices, individual control over personal information, and fair competition.

Privacy regulations should be promulgated to prevent or reduce specific, tangible harms and risk of harm to consumers. Regulations that focus on limiting the collection and retention of data as end goals in and of themselves are unlikely to benefit consumers and may disrupt beneficial innovation, research, and competition. The proposal to set deadlines for data deletion is impracticable and would necessitate the development of expensive technical processes to the advantage of large and technically sophisticated organizations and would foreclose the development beneficial research, innovation, and services. Furthermore, if users wish to return to a service, finding that their data has been deleted would disincentive them from doing so, hampering competition between digital platforms.

CCIA's response to the ACCC's Recommendation 8(e): Increasing Penalties

The ACCC suggests increasing the penalties for breaches of the Privacy Act to mirror the recently increased penalties for breaches of the Australian Consumer Law. Any expansion of civil penalties for privacy violations must be linked to clear principles of enforcement and be supported by economic analysis to ensure that potentially beneficial innovation is not stymied.

If organizations fail to rectify non-compliance with applicable privacy regulations then financial penalties may be appropriate. Financial penalties must strike a balance between the deterrence data misuse and avoiding the suppression of potentially advantageous business practices, innovations, investments, and market entry. Therefore, maximum financial penalties must be rooted in economic analysis tailored to the actual harms or risks-of-harm caused by violations of privacy and security rules. Any proposal to expand maximum penalties should be rooted in economic analysis, rather than an attempt to harmonize different laws.

The ACCC discusses supposed financial benefits of unauthorized uses of data and the potential size of noncompliant organizations to support its recommended increases in maximum penalties for data privacy violations. However, in determining an appropriate penalty for privacy violations, regulators should consider additional factors including the extent and scope of the harm caused by the interference, the sensitivity of the data at issue, and the organization's efforts to rectify the harm or practice.

CCIA's response to the ACCC's Recommendation 8(f): Introducing Direct Rights of Action for Individuals

The ACCC recommends giving individual consumers a direct right to bring actions for breaches of the Privacy Act. CCIA believes that enforcement should be tailored to actual harm or risk of harm and that a private right of action would be unduly burdensome on organizations and divert business resources away from socially beneficial activities.

Lawmakers must strike an appropriate balance between privacy protections and encouraging innovation, investment, and enabling the positive social impacts of big data practices and research. This requires enforcement mechanisms that are proportionate to the risk of harm presented by noncompliant data collection, processing, and disclosure. As the ACCC accurately describes, litigation is expensive and time consuming. A direct right of action would incentivize companies to over-invest in litigation defense to the detriment of developing innovative products, services. Furthermore, the burden of defending suits from individual consumers could be particularly stifling for small companies and new market entrants.

CCIA's response to the ACCC's Recommendation 8(g): Expanding Enforcement Resources

The ACCC recommends providing increased resources to equip the OAIC to deal with increasing volume, significance, and complexity of privacy-related complaints. Additionally the ACCC suggests that it may be appropriate to grant OAIC additional legislative powers to improve its ability to enforce the Privacy Act, such as the power to require publication of notifiable data breaches and steps taken to minimize the risks of harm. CCIA supports appropriate allocation of resources and authority to enable regulatory agencies to fulfill their missions.

In an increasingly data-driven world it is important for data protection authorities to have the resources, staffing, and authority that they require to uphold laws and protect consumer privacy. While complaint investigation and enforcement activities are important tools for rectifying non-compliant data practices, the recommended increase of resources should include the OAIC's information and guidance programs for individuals, businesses, and agencies. These OAIC responsibilities are proactive mechanisms for supporting responsible data stewardship and are important for fostering a healthy environment for consumer privacy.

CCIA's response to the ACCC's Recommendation 9: OAIC Code of Practice for Digital Platforms

The ACCC proposes to recommend that the OAIC to engage with 'key' digital platforms to develop an enforceable code of practice containing specific obligations on how digital platforms must inform consumers and how to obtain consumers' informed consent, as well as appropriate consumer controls over digital platforms' data practices.

Many prominent data-driven companies are raising standards regarding transparency and control over personal information. There is no objective rationale to single out so-called 'key' organizations for participation in and jurisdiction under the proposed Code of Practice. Privacy regulations and obligations should include all organizations that process personal information regardless of whether they have a direct or commercial relationship with an individual whose information they hold. Furthermore, regulations should be sector-neutral, applying to both

online and offline organizations so that businesses and individuals can expect baseline expectations for the treatment of personal data.

Privacy regimes should be outcome-oriented and permit flexibility in compliance in order to promote innovation, competition, and keep up with emerging technologies. Developing "prescribed processes" for duties such as record-keeping and providing notice as contemplated by the ACCC presents significant risks. Overly prescriptive requirements may cause smaller organizations to divert significant resources to record-keeping and compliance instead of developing their products and services. Furthermore, such requirements would prevent businesses throughout the economy from competing to develop new features and controls that better inform and empower consumers.

CCIA's response to the ACCC's Recommendation 10: Serious Invasions of Privacy

The ACCC proposes to recommend that the Government adopt the ALRC's recommendation to introduce a statutory cause of action. In CCIA's view, a private right of action is inappropriate as it would not meaningfully empower ordinary consumers, but would create substantial uncertainty for organizations.

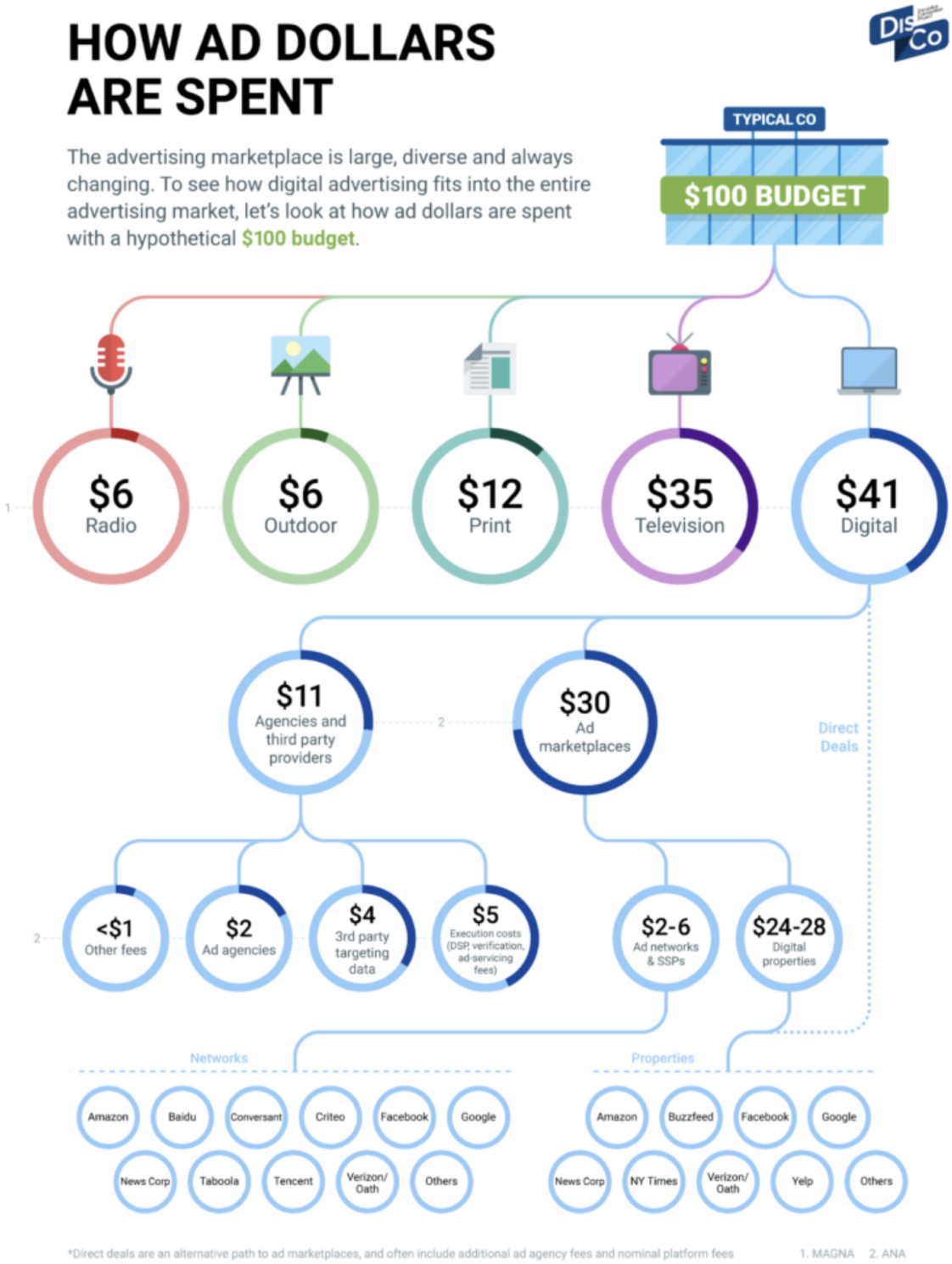
CCIA supports risk-based enforcement for regulating privacy violations. Creating a statutory cause of action would cause organizations to enter a state of perpetual uncertainty, where they would face a risk of enduring costly and time-consuming litigation for even entirely benign activities. While the ACCC raises potential explicit defenses, it is unlikely that these could be sufficiently dispositive at early stages of litigation to allow organizations to avoid significant expenses while facing frivolous suits. Furthermore, permitting the application of fines in situations where actual damage has not occurred is an unbalanced response that will deter investment and chill beneficial business practices, innovation, and services. Finally, it is unclear how a statutory cause of action will give regular consumers meaningfully greater control over their personal information in their interactions with organizations.

CCIA's response to the ACCC's Recommendation 11: Unfair Contract Terms

The ACCC's recommendation that unfair contract terms should be illegal (not just voidable) under the ACL, and that civil pecuniary penalties should apply to their use, would create significant uncertainty for organizations, chilling socially beneficial innovation and data uses.

The ACCC proposes a broad grant of self-power that would create significant uncertainty for organizations, chilling socially beneficial innovation and data uses. Any finding of unfair contract terms that carries financial penalties should be limited to specifically delineated practices or based on clear and predictable principles.

Appendix A:


HOW AD DOLLARS ARE SPENT
The advertising marketplace is large, diverse and always changing. To see how digital advertising fits into the entire advertising market, let's look at how ad dollars are spent with a hypothetical $100 budget.
TYPICAL CO
$100 BUDGET
$6 Radio
$6 Outdoor
$12 Print
$35 Television
$41 Digital
1
$11 Agencies and third party providers
2
$30 Ad marketplaces
Direct Deals
<$1 Other fees
$2 Ad agencies
$4 3rd party targeting data
$5 Execution costs (DSP, verification, ad-servicing fees)
$2-6 Ad networks & SSPs
$24-28 Digital properties
2
Networks
Amazon
Baidu
Conversant
Criteo
Facebook
Google
News Corp
Taboola
Tencent
Verizon/ Oath
Others
Properties
Amazon
Buzzfeed
Facebook
Google
News Corp
NY Times
Verizon/ Oath
Yelp
Others
*Direct deals are an alternative path to ad marketplaces, and often include additional ad agency fees and nominal platform fees
1. MAGNA 2. ANA