ALGORITHMIC COLLUSION AND SCRUTINY: EXAMINING THE ROLE OF THE ACCC'S INFORMATION GATHERING POWERS IN THE DIGITAL ERA

NATHAN FEIGLIN*

An important emerging issue is the fitness-for-purpose of the Australian Competition and Consumer Commission's ('ACCC') information gathering powers given the challenges caused by the proliferation of complex algorithms. This article considers potential harms that may be caused to competition and consumers by (i) algorithms that may assist in creating or enforcing vertical or horizontal restraints; (ii) algorithms that enable self-preferencing by dominant platforms; (iii) algorithms that may facilitate the enforcement of anti-competitive contractual restrictions; and (iv) ranking algorithms that may mislead consumers. After surveying the relevant literature – especially in relation to the potential harms of horizontally collusive algorithms – and the state of the ACCC's information gathering powers under section 155(1) of the Competition and Consumer Act 2010 (Cth), this article proposes an additional two technology-based information gathering powers, including the power for the ACCC to scrutinise algorithms.

I INTRODUCTION

This article seeks to address the risks of competitive or consumer harm being caused by the use of algorithms that may restrain competition or mislead consumers. In July 2019, the final report of the Australian Competition and Consumer Commission's ('ACCC') Digital Platforms Inquiry ('*DPI Final Report*') recommended a 'specialist digital platforms branch'[1] within the ACCC, with a purpose including 'proactively monitoring and investigating instances of

* LLB (Hons); Graduate at the Australian Competition and Consumer Commission ('ACCC'). An earlier version of this article was submitted as a Research Thesis at the University of Technology Sydney. I am grateful for the supervision of Emeritus Professor Jill McKeough, and the feedback of Dr Rob Nicholls, Adrian Coorey, the anonymous reviewers, and the editorial team. Errors are my own. The views in this article are solely mine and are not those of the ACCC.

1 Australian Competition and Consumer Commission, *Digital Platforms Inquiry* (Final Report, June 2019) 31 <https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf> ('*DPI Final Report*').

potentially anti-competitive conduct and conduct causing consumer harm by digital platforms'.[2]

This article aims to make an original contribution to the literature on four bases. First, in the evaluation of the fitness-for-purpose of the ACCC's investigative powers in the digital era. Second, in the analysis of the application of established regulatory theory in contemporary contexts. Third, by proposing a novel 'application programming interface'-based investigatory mechanism wherein the ACCC is empowered to proactively audit, experiment with, and test algorithms in order to understand and determine their potential or actual harms. Fourth, through the proposal of a similar technological protocol to the third contribution to enable the ACCC to proactively or reactively 'poll' for documents and information that may be relevant to the investigation of possible contraventions of the *Competition and Consumer Act 2010* (Cth) ('*CCA*') or the *Australian Consumer Law*.[3]

Part II provides background to the issues, including how algorithms may tacitly collude and be used in resale price maintenance, and how search algorithms may mislead consumers in their rankings and enforce conditions that restrict competition. Part III discusses the risks and responses to collusive algorithms in-depth. Part IV analyses relevant regulatory compliance theory and practice. Part V evaluates the fitness-for-purpose of the ACCC's current information gathering powers for proactive enforcement. Part VI proposes a new technical investigation and monitoring mechanism to address algorithmic harms. Part VII is the conclusion.

II BACKGROUND

Describing the recommended digital platforms branch, ACCC Chairman Rod Sims described one of its functions as being the execution of experiments on the algorithms of Google and Facebook to determine if they cause consumer or competitive harm. Sims stated that the branch will:

> be testing [the] Facebook and Google algorithms to see whether there's any anti-competitive or misleading behaviour. We can do that by throwing a lot of things at those algorithms. If we find things that we're unclear of then we'd have the ability to get information from the digital platforms.[4]

This article considers the ACCC's compulsory information gathering powers under sections 155 and 95ZK of the *CCA* and considers a technological and legal model under which the ACCC would be empowered to test algorithms for anti-competitive effects (the 'algorithm scrutiny power') and proactively poll for data that could reveal anti-competitive or other prohibited conduct (the 'data request

2 Ibid.

3 *Competition and Consumer Act 2010* (Cth) sch 2 ('*Australian Consumer Law*').

4 ACCCgovau (Australian Competition and Consumer Commission), 'Digital Platforms Inquiry [Press Conference]' (YouTube, 25 July 2019) 00:16:26–00:16:53 <https://www.youtube.com/watch?time_continue=2225&v=Fsu4dQbHKOc> ('Digital Platforms Inquiry').

power'). This proposal has significant pertinence alongside emerging literature that indicates that algorithms may collude,[5] and that algorithms may be used to monitor and enforce vertical price restraints.[6] Additionally, analysis of pricing and sales data may be used in the detection of cartel conduct and concerted practices. This proposal highlights and addresses the unduly limited scope of the Digital Platforms Inquiry recommendation of proactive monitoring and enforcement.[7]

A Rise of Algorithms and Data

This section introduces and discusses the broad scale of algorithm usage, as well as categories of potential competitive or consumer harm that may be caused by algorithms.

The law has long been recognised as lagging behind technological innovation.[8] Access to technology, data and the internet has fuelled economic opportunity and increased efficiency.[9] However, in more recent times, regulators have become aware of potential competitive concerns that may arise from the increase in price (and other non-price variable) transparency that is enabled by digital technologies, and the ability for firms to hastily react to market conditions, including the actions of their competitors.[10] At the same time, new competitive concerns have been raised about the conduct of dominant digital platforms.[11] The same has held true for web-based intermediary businesses that function as 'vertical search' providers, such as online travel agents ('OTAs'). Below, three risks of harm are described which illustrate the importance of regulators having fit-for-purpose investigatory powers and protocols that enable them to identify and intervene in cases of competitive or consumer harm. Then, the risks of and responses to algorithmic collusion are advanced throughout the article.

1 Algorithms May Collude and Assist in Vertical Restraint Enforcement

'Algorithmic pricing' is the use of software algorithms to set the price of goods or services. It is possible that algorithms may be programmed to collude on price or non-price variables or self-learn how to collude.[12]

---

5 See, eg, Ariel Ezrachi and Maurice E Stucke, 'Artificial Intelligence & Collusion: When Computers Inhibit Competition' [2017] (5) *University of Illinois Law Review* 1775 ('AI Collusion').

6 See, eg, Rob Nicholls, 'Lessons for Australia in the EU's Algorithmic Price War That Ripped Off Consumers', *The Conversation* (online, 30 July 2018) <http://theconversation.com/lessons-for-australia-in-the-eus-algorithmic-price-war-that-ripped-off-consumers-100607>.

7 *DPI Final Report* (n 1) 140–1.

8 See, eg, Lyria Bennett Moses, 'Agents of Change: How the Law "Copes" with Technological Change' (2011) 20(4) *Griffith Law Review* 763.

9 See, eg, James Manyika and Charles Roxburgh, *The Great Transformer: The Impact of the Internet on Economic Growth and Prosperity* (Report, October 2011) <https://www.mckinsey.com/~/media/McKinsey/Industries/High%20Tech/Our%20Insights/The%20great%20transformer/MGI_Impact_of_Internet_on_economic_growth.ashx>; Alice M Rivlin and Robert E Litan, *The Economy and the Internet: What Lies Ahead?* (Report, 1 December 2001) <https://www.brookings.edu/research/the-economy-and-the-internet-what-lies-ahead/>.

10 Ezrachi and Stucke, 'AI Collusion' (n 5) 1797–9.

11 See generally *DPI Final Report* (n 1).

12 Ariel Ezrachi and Maurice E Stucke, *Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy* (Harvard University Press, 2016) pt II ('Virtual Competition').

In their empirical analysis of algorithmic pricing on Amazon Marketplace, Chen, Mislove and Wilson find that while algorithmic pricing may increase seller revenue,[13] such mechanisms may be implemented to collude, and may also lead to 'unexpected' results.[14] They cite an example where two competing algorithms resulted in a textbook being priced in excess of USD23 million.[15] It has been posited that algorithms control the majority of the 2.5 million daily price changes on Amazon.[16] This author located a service that advertised its ability to price dynamically[17] and optimise pricing for profit.[18] The same service also appeared to allow its users to monitor compliance with their suggested retail price or resale price maintenance policies.[19] The European Commission fined four consumer electronics manufacturers a total of EUR 111 million for resale price maintenance.[20] In those cases,

> [m]anufacturers were using algorithmic price monitoring to figure out when retailers were discounting prices, while the same retailers were using algorithms to increase the competitiveness of their pricing.[21]

Nicholls sees an opportunity for the ACCC to utilise algorithmic tools to detect anti-competitive conduct.[22]

While online markets intuitively come to mind when considering algorithmic pricing, the technology has also been emerging in offline retail markets. For example, supermarkets in Australia[23] and the United Kingdom ('UK')[24] have trialled digital price tags that could be updated by software at a far faster rate than by hand.

---

13 Le Chen, Alan Mislove and Christo Wilson, 'An Empirical Analysis of Algorithmic Pricing on Amazon Marketplace' (Conference Paper, International World Wide Web Conference, April 2016) 1339, 1348 <https://mislove.org/publications/Amazon-WWW.pdf>.

14 Ibid 1339.

15 Michael Eisen, 'Amazon's $23,698,655.93 Book about Flies', *it is NOT junk* (Blog Post, 22 April 2011) <http://www.michaeleisen.org/blog/?p=358>.

16 'Profitero Price Intelligence: Amazon Makes More than 2.5 Million Daily Price Changes', *Profitero Blog* (Blog Post, 10 December 2013) <https://www.profitero.com/2013/12/profitero-reveals-that-amazon-com-makes-more-than-2-5-million-price-changes-every-day/>.

17 'Dynamic Pricing Software', *Prisync* (Web Page) <https://prisync.com/platform/dynamic-pricing.html>.

18 'Price Optimization Software', *Prisync* (Web Page) <https://prisync.com/platform/ecommerce-pricing-optimization.html>.

19 'Minimum Advertised Price Monitoring Software', *Prisync* (Web Page) <https://prisync.com/platform/map-monitoring-software.html>.

20 European Commission, 'Antitrust: Commission Fines Four Consumer Electronics Manufacturers for Fixing Online Resale Prices' (Press Release No IP/18/4601, 24 July 2018) <https://europa.eu/rapid/press-release_IP-18-4601_en.htm>.

21 Nicholls (n 6).

22 Ibid.

23 Dominic Powell, 'Supermarkets Shoot Down Claims Grocery "Surge Pricing" Is in the Works, but Could Digital Tickets Be a Win for Retailers?', *SmartCompany* (online, 3 July 2017) <https://www.smartcompany.com.au/industries/retail/supermarkets-shoot-claims-grocery-surge-pricing-works-digital-tickets-win-retailers/>; Olivia Lambert, 'Woolworths Trialled Electronic Ticketing System in Schofields Store', *News.com.au* (online, 30 June 2017) <https://www.news.com.au/finance/business/retail/woolworths-trialled-electronic-ticketing-system-in-schofields-store/news-story/2dcb8fab97f773ac01209a9454a49f3f>.

24 Elanor Lawrie, 'Why Your Bananas Could Soon Cost More in the Afternoon', *BBC News* (online, 30 June 2017) <https://www.bbc.com/news/business-40423114>.

Under the algorithm scrutiny power proposed in this article, regulators will be better empowered to understand and take action against potentially harmful horizontal or vertical restraints enforced by algorithms through the ability to more closely scrutinise them.

2 Platforms May Self-Preference

Self-preferencing is where a platform firm uses its market power to give itself a competitive advantage over rivals on its platform,[25] or rivals within its technology or business ecosystem. This was illustrated in the European Commission *Google Shopping* decision.[26] As Holzweber summarised, in that decision:

> [t]he claim was that Google gave its own services an illegal advantage by placing them more favourably in the search engine results than other services. While Google's own comparison shopping service was placed at the top of the search results, Google's competitors were on average placed on page four of the search results.[27]

The ACCC provides additional examples of alleged and potential self-preferencing conduct in the *DPI Final Report*.[28] In response to self-preferencing concerns in search results, a 'search neutrality' principle has been proposed. However, it has been argued that implementing it would hamper innovation.[29] Hyman and Franklyn found that making a Google search prominently link to rival vertical search services was more effective than making Google clearly label its own vertical search (that is, Google Shopping) results in increasing the click through rates to rival specialised search services.[30] Thus, they argue that 'architectural remedies' as opposed to 'labelling remedies' may have the greatest impact in cases of self-preferencing.[31]

An algorithm may be programmed to self-preference. For example, by being programmed to rank some categories or results higher than others. In the future, through machine learning, it may be possible that an algorithm not explicitly programmed to self-preference will eventually self-preference if it learns that self-preferencing assists it in achieving its specified goal.[32] This goal may be to increase overall firm profitability.

Without the ability to inspect and test opaque algorithms, regulators are severely restricted in their ability to understand how consumer harms are or may

---

25 See Damien Geradin and Dimitrios Katsifis, 'An EU Competition Law Analysis of Online Display Advertising in the Programmatic Age' (2019) 15(1) *European Competition Journal* 55, 90.

26 *Commission Decision of 27 June 2017 Relating to Proceedings under Article 102 of the Treaty on the Functioning of the European Union and Article 54 of the Agreement on the European Economic Area (Case AT.39740 – Google Search (Shopping))* [2018] OJ C 61/11.

27 Stefan Holzweber, 'Tying and Bundling in the Digital Era' (2018) 14(2–3) *European Competition Journal* 342, 346 (citations omitted).

28 *DPI Final Report* (n 1) 133–6.

29 Daniel A Crane, 'Search Neutrality and Referral Dominance' (2012) 8(3) *Journal of Competition Law and Economics* 459, 467.

30 David A Hyman and David J Franklyn, 'Search Bias and the Limits of Antitrust: An Empirical Perspective on Remedies' (2014) 55(3) *Jurimetrics Journal of Law, Science and Technology* 339.

31 Ibid 376.

32 See generally Ezrachi and Stucke, 'AI Collusion' (n 5) 1783.

be occurring, and to enforce – or consider advocating for the reform of – competition and consumer protection laws.

3 Potentially Anti-competitive Contractual Clauses May Be Enforced by Vertical Search Result Rankings and Vertical Search Providers May Mislead Consumers

As foregrounded above, the ranking of content is a novel area of interest for regulators in online markets.[33] Unless the position of online content is manually curated by a human, algorithms control its ranking and display.[34] A particular area of attention for regulators over the past five years has been how OTAs utilise 'most favoured nation' ('MFN') clauses in their dealings with hotels. Of novel concern is how the ranking of hotels within OTAs' search results may be used to enforce compliance with MFN clauses by ranking a non-compliant hotel lower in default search results. The law and economics around MFN clauses have been the subject of considerable debate.[35]

Generally, a MFN or 'price parity' clause exists in contracts wherein the covenantor (for example, the hotel) agrees not to provide a good or service through another channel at a price lower than the price for the equivalent good or service offered through the covenantee's channel (for example, the OTA the hotel is contracting with). Under a so-called 'wide' price parity clause in OTAs' agreements, a hotel cannot provide a cheaper price for the same room through its own website, call centre or in-person booking process than through that OTA.[36] The hotel also generally must not offer a room category that is not offered through its OTA channel through its other sales channels.

Contrastingly, a 'narrow' price parity clause generally allows the hotel to offer a lower price to consumers that telephone call the hotel directly, seek to make an in-person walk-in booking, or are members of the hotel's loyalty program.[37]

Globally, competition regulators and lawmakers have taken varying amounts of action, resulting in outcomes ranging from banning price parity clauses altogether, or just limiting their use to 'narrow' clauses.[38] It is noted that the economic theory of harm commonly adopted by regulators 'that price parity clauses limit competition between platforms on commission rates, ultimately leading to higher prices being charged to consumers'[39] has not been directly

33 See generally Jonathan B Baker and Fiona Scott Morton, 'Antitrust Enforcement against Platform MFNs' (2018) 127(7) *Yale Law Journal* 2176.

34 See, eg, 'All You Need to Know about Ranking, Search Results and Visibility', *Booking.com* (Web Page, 16 July 2020) <https://partner.booking.com/en-gb/help/growing-your-business/all-you-need-know-about-ranking-search-results-and-visibility>; 'How Search Algorithms Work', *Google Search* (Web Page) <https://www.google.com/search/howsearchworks/algorithms/>.

35 See, eg, Baker and Scott Morton (n 33); Pinar Akman and D Daniel Sokol, 'Online RPM and MFN under Antitrust Law and Economics' (2017) 50(2) *Review of Industrial Organization* 133.

36 'What's Happening with Rate Parity in the Hotel Industry?', *Trivago Business Blog* (Blog Post, 14 March 2019) <https://businessblog.trivago.com/rate-parity-hotel-industry-status/>.

37 Ibid.

38 See Thibaud Vergé, 'Are Price Parity Clauses Necessarily Anticompetitive?' (22 January 2018) *CPI Antitrust Chronicle* 3 <https://dev.competitionpolicyinternational.com/are-price-parity-clauses-necessarily-anticompetitive/>; Baker and Scott Morton (n 33).

39 Vergé (n 38) 3.

tested.[40] However, in Italy and France, the banning of price parity clauses was found to lead to a 'significant reduction' in room prices in the medium-term.[41]

Hunold, Kesler and Laitenberger suggest that the default rankings of results by OTAs are based on factors which are relevant to the likelihood of the agent maximising its profit, as opposed to meeting the needs of searching consumers.[42]

Price parity may be enforced contractually, but there is emerging evidence of the practice being enforced or encouraged through algorithmic software. For example, where hotels that do not conform to price parity are ranked lower in search results by OTAs.[43] Large OTA Expedia is one such OTA that has acknowledged engaging in this practice.[44]

Under a slightly different ranking scenario, albeit with the same profit-maximisation objective, the ACCC successfully took enforcement action under sections 18, 29 and 34 of the *Australian Consumer Law* against OTA Trivago for allegedly ranking hotel results based on what it would earn for each click on a hotel room result when the consumer was led to believe by television advertisements and the design of Trivago's website that Trivago was assisting them in identifying the cheapest hotel room prices.[45]

In September 2018, the ACCC said it was again investigating the competitive effects of price parity agreements.[46]

It is argued that the proposed algorithm scrutiny power would enable regulators to better understand the inputs and effects of algorithms, such as ranking algorithms, within the context of their investigations and inquiries.

---

40 Ibid 5.

41 Andrea Mantovani, Claudio A Piga and Carlo Reggiani, 'Much Ado about Nothing? Online Platform Price Parity Clauses and the EU Booking.com Case' (Discussion Paper No 1909, University of Manchester, 28 May 2019) 1 <http://dx.doi.org/10.2139/ssrn.3381299>.

42 Matthias Hunold, Reinhold Kesler and Ulrich Laitenberger, 'Hotel Rankings of Online Travel Agents, Channel Pricing and Consumer Protection' (Discussion Paper No 300, Düsseldorf Institute for Competition Economics, September 2018) 3 <http://www.dice.hhu.de/fileadmin/redaktion/Fakultaeten/Wirtschaftswissenschaftliche_Fakultaet/DICE/Discussion_Paper/300_Hunold_Kesler_Laitenberger.pdf>.

43 Daniel Mandrescu, 'The Return of the MFN Clauses – Platform Ranking as an Enforcement Mechanism for Price Parity', *Lexxion* (Blog Post, 26 June 2019) <https://www.lexxion.eu/en/coreblogpost/the-return-of-the-mfn-clauses-platform-ranking-as-an-enforcement-mechanism-for-price-parity/>.

44 Matthew Elmas, 'Expedia Will Allow Hotels to Undercut Its Prices Online, but Threatens to Shaft Those That Do', *SmartCompany* (online, 25 March 2019) <https://www.smartcompany.com.au/business-advice/competition/expedia-allow-hotels-undercut-prices-online/>.

45 *Australian Competition and Consumer Commission v Trivago NV* (2020) 142 ACSR 338.

46 Naaman Zhou, 'Australians Told to Call Hotels, Rather than Rely on Booking Sites, for Cheaper Rates', *The Guardian* (online, 15 September 2018) <https://www.theguardian.com/travel/2018/sep/15/australians-told-to-call-hotels-rather-than-rely-on-booking-sites-for-cheaper-rates>.

III COLLUSIVE PRICING ALGORITHMS: RISKS AND RESPONSES

A Background

This Part further advances the discussion of potentially collusive algorithms as introduced in Part II and finds that while the liability rules are unsettled, further investigation should be undertaken.

It is uncontroversial that increased price transparency which can be processed through algorithms may raise collusion concerns which, if materialised, could decrease consumer welfare.[47]

The potential risks of collusion are real. For example, in a simplified pricing game example using a 'Q-learning' self-learning algorithm,[48] Calvano et al found that it was possible for algorithms to converge to cooperative action up to 95% of the time.[49] The authors considered that under a real-world environment, the challenges of maintaining 'stability, adaption, and scalability' may reduce the amount of convergence that can be achieved between firms.[50] However, the authors further noted that pricing algorithms used in practice are likely to benefit from the latest artificial intelligence developments as opposed to their simplified Q-learning simulation.[51] Ittoo and Petit also provide a detailed discussion of Q-learning and reinforcement learning more generally.[52]

B Ezrachi and Stucke's Typology

In order to comprehend the types of harm that may result from collusive algorithms, this article adopts Ezrachi and Stucke's four scenario typology, adapted below (inspired by Nicholls and Fisse),[53] where collusive conduct ranges from being human-driven but using technology to facilitate a cartel agreement under their 'Messenger Scenario', to being almost completely led by multiple firms adopting predictive or self-learning algorithms under their 'Predictable Agent' and 'Digital Eye' scenarios, respectively.[54] The empirical evidence-base behind this typology is limited, with the authors criticised for potentially overstating the risks of collusion under their scenarios.[55]

---

47 Ariel Ezrachi and Maurice E Stucke, 'Algorithmic Collusion: Problems and Counter-Measures' (Discussion Paper, OECD Competition Committee, 21 June 2017) 18–19 [68]–[70] <https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DAF/COMP/WD%282017%2925&docLanguage=En>.

48 See Christopher JCH Watkins and Peter Dayan, 'Q-Learning' (1992) 8(3) *Machine Learning* 279.

49 Emilio Calvano et al, 'Algorithmic Pricing What Implications for Competition Policy?' (2019) 55(1) *Review of Industrial Organization* 155, 165.

50 Ibid 164–5.

51 Ibid 166.

52 Ashwin Ittoo and Nicolas Petit, 'Algorithmic Pricing Agents and Tacit Collusion: A Technological Perspective' in Hervé Jacquemin and Alexandre De Streel (eds), *L'intelligence Artificielle et le Droit* (Larcier, 2017) 241.

53 Rob Nicholls and Brent Fisse, 'Concerted Practices and Algorithmic Coordination: Does the New Australian Law Compute?' (2018) 26(1) *Competition and Consumer Law Journal* 82, 86–7.

54 Ezrachi and Stucke, 'AI Collusion' (n 5) 1782–3.

55 Nicholls and Fisse (n 53) 87.

Table 1: Typology Adapted from Ezrachi and Stucke's Algorithmic Collusion Scenarios[56]

Scenario	Description
Messenger	A computer or algorithm is used to give effect to a separately concluded cartel agreement.[57]
Hub & Spoke	A single algorithm is used to determine the prices offered by multiple users.[58]
Predictable Agent	Algorithms are implemented by firms to respond to market conditions in a pre-programmed way.[59] They may be developed with awareness of algorithms likely to be implemented by competitors.[60]
Digital Eye	Self-learning algorithms are implemented by firms and set an objective.[61] Each algorithm experiments and determines the means through which the objective is met.[62]

Under the Messenger Scenario, giving effect to a 'contract, arrangement, or understanding'[63] is likely to contravene part IV division 1 of the *CCA* and attract per se liability.[64] The *CCA* section 155 power may be invoked by investigators to seek documents which may contain written evidence of a cartel provision or written notes describing how computers may have been used to implement the cartel. The *CCA* section 155 powers are further explained in Part V of this article. Computer source code may also be compelled, given the expansive definition of 'documents' under the *CCA*.[65] Under the Messenger Scenario, there is likely to be more documentary evidence that would exist under 'traditional' cartel arrangements than when compared to the Predictable Agent and Digital Eye scenarios.

C Concerted Practices and Collusive Algorithms

Failing the existence of evidence that could point to a 'contract, arrangement, or understanding',[66] the prohibition on concerted practices under section 45(1)(c) of the *CCA* is the next most relevant potential source of liability for colluding algorithms. Liability under the provision requires that a corporation (or person[67]) 'engage[s] with one or more [other] persons in a concerted practice that has the

56 Ibid 1781–96.
57 Ezrachi and Stucke, 'AI Collusion' (n 5) 1782.
58 Ibid.
59 Ibid 1783.
60 Ibid.
61 Ibid.
62 Ibid.
63 *Competition and Consumer Act 2010* (Cth) s 45AD ('*CCA*').
64 Ibid ss 45AG, 45AK.
65 Ibid s 4 (definition of 'document').
66 Ibid s 45AD.
67 Ibid sch 1 s 45(1)(c).

purpose, or has or is likely to have the effect, of substantially lessening competition'.[68]

The prohibition has not yet been litigated. In February 2019, ACCC Chair Rod Sims stated that he was confident that the regulator would bring proceedings under section 45(1)(c) that year.[69] In December 2019, the ACCC announced its acceptance of enforceable undertakings in relation to concerns under that provision caused by posts in a Facebook group seeking to increase roofing services prices in Sydney.[70] A number of authors have comprehensively considered how the provision may be applied.[71] Relevantly, Davies and Wainscoat note that firms developing or implementing self-learning pricing algorithms should document their decisions in order 'to avoid [the] inference of [an] anti-competitive purpose'.[72] Gvozdenovic has argued that the 'proper' interpretation of section 45(1)(c) may prove ineffective in achieving the ACCC's enforcement objectives.[73]

Nicholls and Fisse find that even if there is anti-competitive intent in the design or creation of a Predictable Agent pricing algorithm, their usage will not attract liability under *CCA* section 45(1)(c) due to their 'unilateral nature'.[74] Comparably, they find that *CCA* section 45(1)(c) will be unlikely to capture 'Digital Eye'-type algorithms, due to their unilateral nature, as well as questioning whether a corporation can 'engage in' conduct required to establish a 'concerted practice' without the action nor assent of a human agent.[75] However, in Europe, Colombo has commented that 'the antitrust watchdog will not be willing to hear defendants ceaselessly denying any relationship and responsibilities between them and the computer'.[76] It is possible that such an approach may be adopted in Australia, once section 45(1)(c) is tested in the courts.

D Other Proposals

Internationally, bodies and academics have suggested measures to address potential harms to competition from algorithms. While commentators have

68 Ibid.

69 Rod Sims, '2019 Compliance and Enforcement Policy' (Speech, Committee for Economic Development Australia, 26 February 2019) <https://www.accc.gov.au/speech/2019-compliance-and-enforcement-policy>.

70 Australian Competition and Consumer Commission, 'Sydney Hailstorm Described as "Perfect Opportunity" to Increase Prices' (Media Release No 237/19, 11 December 2019) <https://www.accc.gov.au/media-release/sydney-hailstorm-described-as-%E2%80%98perfect-opportunity%E2%80%99-to-increase-prices>.

71 See, eg, Michael Gvozdenovic, 'Concerted Practices and Statutory Interpretation: An Affirmation of the Jurisprudence on "Contracts, Arrangements and Understandings"' (2019) 26(3) *Competition and Consumer Law Journal* 213; Caitlin Davies and Luke Wainscoat, 'Not Quite a Cartel: Applying the New Concerted Practices Prohibition' (2017) 25(2) *Competition and Consumer Law Journal* 173; Rob Nicholls and Deniz Kayis, 'Concerted Practices Contested: Evidentiary Thresholds' (2017) 25(2) *Competition and Consumer Law Journal* 125.

72 Davies and Wainscoat (n 71) 213.

73 Gvozdenovic (n 71) 237.

74 Nicholls and Fisse (n 53) 98.

75 Ibid 100.

76 Niccolò Colombo, 'Virtual Competition: Human Liability Vis-à-Vis Artificial Intelligence's Anticompetitive Behaviours' (2018) 2(1) *European Competition and Regulatory Law Review* 11, 14.

suggested numerous possible responses, this Part finds that many of them rest on untested assumptions and indicate the need for further evidence.

1 Per Se Liability for Collusive Self-Learning Algorithms

Harrington considers a hypothetical scenario wherein two firms adopt a self-learning algorithm that, with a profit maximisation target, adjusts prices 'until they are using the sort of pricing rule that firms deploy when colluding'.[77] This scenario is similar to Ezrachi and Stucke's Digital Eye, as discussed above.[78] Harrington then postulates a definition of 'collusion' as being 'when firms use strategies that embody a reward-punishment scheme which rewards a firm for abiding by the supracompetitive outcome and punishes it for departing from it'.[79]

Harrington finds that tacit collusion will not violate the *Sherman Antitrust Act of 1890*[80] nor article 101(1) of the *Treaty of the Functioning of the European Union*[81] due to the lack of 'mutual understanding among firms that they will restrict competition in some manner'.[82] He notes that successful claims in United States and European Union jurisdictions typically required evidence of overt communication between firms.[83] In Australia, it appears highly probable that evidence of communication will be required to establish a concerted practice.[84] This type of evidence will not be available when each firm separately selects or develops and implements their own pricing algorithm. Given this limitation in evidence, Harrington postulates that per se liability should attach to pricing algorithms that have certain anti-competitive properties.[85] He proposes that liability be determined by examination of an algorithm's source code, or by inputting data into the algorithm and monitoring its output.[86]

Harrington finds that the efficiency gains that are promoted by pricing algorithms are unlikely to be lost by a prohibition on certain collusive algorithms because

> [a]n [artificial pricing agent] is "not collusive" if its price recommendation is not dependent on rival firms' responding in a particular manner; for example, a price increase is not contingent on rival firms subsequently matching that price, or maintaining price is not contingent on rival firms conducting a price war if price were to be reduced.[87]

---

77 Joseph E Harrington, 'Developing Competition Law for Collusion by Autonomous Artificial Agents' (2018) 14(3) *Journal of Competition Law and Economics* 331, 332.
78 Ezrachi and Stucke, 'AI Collusion' (n 5) 1782–3.
79 Harrington (n 77) 336.
80 15 USC § 1 (2018).
81 *Treaty on the Functioning of the European Union,* opened for signature 25 March 1957, [2012] OJ C 326/47 (entered into force 1 January1958) ('*FEU*').
82 Harrington (n 77) 337.
83 Ibid 338.
84 Davies and Wainscoat (n 71) 180.
85 Harrington (n 77) 350–1.
86 Ibid 351.
87 Ibid 357.

Further, Harrington argues that because 'far too little' is known about algorithmic collusion, no approach should be dismissed, with a per se prohibition the only currently viable approach.[88]

Per se liability may be preferable to a 'substantial lessening of competition' test because of the practical difficulties of establishing a counterfactual when determining harm,[89] in addition to the obscurity of what is meant by a 'substantial' lessening of competition both generally and in this context. In *Radio 2UE Sydney Pty Ltd v Stereo FM Pty Ltd*, Lockhart J observed the word 'substantial' to be 'imprecise and ambiguous'.[90] This imprecision was again recognised this year.[91]

2 Other Measures

Ezrachi and Stucke consider various ideas in response to their identified challenges arising from pricing algorithms. A non-exhaustive summary of their proposals and relevant critiques are provided below.

First, the authors consider that a market inquiry or investigation initiated by a competition regulator in order to understand possible harms would be beneficial.[92] This has been broadly supported, including by the Organisation for Economic Co-operation and Development ('OECD'), and Colombo – as detailed below.

Second, they consider proposing that liability is imposed once a defendant becomes aware its algorithm is coordinating with would-be competitors.[93] They suggest that such liability could be modelled on the *Proceeds of Crime Act 2002* (UK), where liability is imposed where a person is aware that they are dealing with proceeds of crime. Therefore, liability could attach to a person when they become aware that their algorithm is exhibiting anti-competitive effects. However, they note practical difficulties with defining and enforcing liability in such an instance. Specifically, they note that perception of coordination could be conflated with other variables that an algorithm could control to boost profits, such as reducing costs or strategic discounting.[94] Further, they consider that even if an individual became aware of such collusion, there may be little that they are able to do to intervene.[95]

Third, they note that a regulator could impose a time delay on algorithmic price changes. However, this would have the impact of slowing discounting.[96] They then consider that the delay could just be imposed on price increases, however, this is dismissed as suboptimal because it could unintentionally stimulate further tacit collusion.[97]

---

88 Ibid 358.
89 Ezrachi and Stucke, *Virtual Competition* (n 12) 222.
90 (1982) 62 FLR 437, 444.
91 *Australian Competition and Consumer Commission v Pacific National Pty Ltd* (2020) 378 ALR 1, 25 [104], 60 [219] (Middleton and O'Bryan JJ).
92 Ezrachi and Stucke, 'AI Collusion' (n 5) 1806.
93 Ibid 1804.
94 Ibid.
95 Ibid.
96 Ibid 1805.
97 Ibid 1805–6; Ezrachi and Stucke, *Virtual Competition* (n 12) 229–30.

Fourth, they consider a proposal whereby an enforcement agency may 'audit' firm algorithms to examine them for possible anti-competitive effects and to inform potential government-backed countermeasures to such potential effects.[98] However, they note several potential practical drawbacks to their proposal. First, they consider that algorithms are unlikely to display a straightforward 'collusive' purpose or effect in their source code.[99] Second, they note that running the algorithms in a limited sandbox environment may not display their full effects, as opposed to when they are deployed in a live market environment.[100] Third, they consider that designing and implementing an appropriate remedy (if justified), would be challenging. They note that a remedy that would reduce the potential efficiency achievable through data sharing between suppliers and customers or by combining multiple datasets, may lead to a suboptimal outcome. Finally, they note that technical limitations may hamper the ability for useful auditing to take place or the development or implementation of adequate market countermeasures. They also find that any such countermeasures are unlikely to 'keep pace' with the potentially increasing complexity and quality of algorithms deployed by market participants.[101] They do remark, however, that auditing may become increasingly feasible as the technology capability of regulators increases over time.[102] More recently, the impact of these drawbacks has been questioned by Colombo.[103]

The OECD has proposed consideration of three categories of measures to address possible harms.[104] First, that market studies and market investigations are used to investigate whether market failure is arising and to identify – or in the case of investigations, mandate – solutions.[105] Second, that merger control intervention thresholds are reduced in markets with algorithmic activity that may facilitate collusion. They posit that this should apply even in less concentrated markets that would not usually attract merger scrutiny by a regulator, with attention paid to market transparency and 'velocity of interaction'.[106] Finally, the authors propose that regulators could seek behavioural commitments from firms with a large degree of market power in concentrated markets. The commitments could include to refrain from engaging in certain algorithmic activities, in addition to enabling the auditing of their algorithm programming and usage.[107] Gal and Elkin-Koren consider that a 'well thought [out]' remedy may be required to address oligopolistic coordination, which that may be made more durable through algorithm usage.[108]

98 Ezrachi and Stucke, *Virtual Competition* (n 12) 230.
99 Ibid.
100 Ibid 230–1.
101 Ibid 231.
102 Ibid.
103 Colombo (n 76) 20.
104 Organisation for Economic Co-operation and Development, *Algorithms and Collusion: Competition Policy in the Digital Age* (Report, 14 September 2017) 40–2 <https://www.oecd.org/competition/algorithms-collusion-competition-policy-in-the-digital-age.htm>.
105 Ibid 40.
106 Ibid 41.
107 Ibid 42.
108 Michal S Gal and Niva Elkin-Koren, 'Algorithmic Consumers' (2017) 30(2) *Harvard Journal of Law and Technology* 309, 347.

Calvano et al propose four possible policy approaches.[109] First, maintaining current policy approaches. This rests upon the 'optimistic' assumption that pricing algorithms do not pose any novel problems.[110] Second, the authors propose *ex ante* regulation of pricing algorithms. They refer to Ezrachi and Stucke's proposal of an algorithm 'sandbox',[111] as well as Harrington's consideration of per se liability – as discussed above. Third, *ex post* intervention but with 'different legal standards'.[112] Finally, they consider, but determine suboptimal, an 'outright prohibition on algorithmic pricing'.[113]

Colombo lists numerous hypothetical market-based and regulatory solutions.[114] The author's *ex ante* measures include: [115]

- mandatory 'antitrust compliance by design' standards to be adhered to by developers;
- kill switch mechanisms to enable human intervention if self-learning algorithms circumvent programmatic safeguards implemented by developers;
- 'auditing mechanism for algorithms';
- increased 'merger control … in markets with algorithmic activities'; and
- 'counter algorithms aimed at limiting speed and frequency with which market players may adjust prices'.

Colombo's *ex post* proposals include countermeasures that fight 'technology with technology' including that:

- consumers use 'digital butlers' to increase their buyer power by 'find[ing] alternative paths to collusion';[116] and
- competition regulators 'put into place increasingly effective forensic tools' in order to 'detect unusual market trends stemming from algorithm-driven strategies'.[117]

Further, Colombo agrees with Ezrachi and Stucke's[118] proposal that competition regulators instigate market studies and market investigations to 'understand the dynamics [that] lead to collusion' before proposing intervention.[119]

3 Regulatory Double Bind Justifies at Least Market Inquiry or Investigation

Colombo warns of a regulatory 'double bind' that arises because of the difficulty of determining whether to intervene in markets (and the extent of any

109 Calvano et al (n 49) 167–9.
110 Ibid 168.
111 Ezrachi and Stucke, *Virtual Competition* (n 12) 230–1.
112 Calvano et al (n 49) 168.
113 Ibid.
114 Colombo (n 76) 20–1.
115 Ibid 20.
116 Ibid 21.
117 Ibid.
118 Ezrachi and Stucke, 'AI Collusion' (n 5) 1806.
119 Colombo (n 76) 21.

such intervention), because the harms 'cannot be easily predicted'[120] until the technology is widespread. However, at the point that technology becomes widespread, intervention may become substantially more difficult.[121]

While it is challenging to formulate evidence-based policy in a dynamic and uncertain digital environment, the technology-based proactive investigative powers, especially the algorithm scrutiny power, proposed in Part VI of this article will assist the ACCC in understanding the potential harms. Once a response is determined, those powers can be engaged through enforcement investigations – vital under a classical criminological model, predicated on deterring wrongdoing.[122] The next Part of this article considers relevant regulatory theory, practice, and reasons for compliance.

IV ANALYSIS OF RELEVANT REGULATORY THEORY AND PRACTICE

While the primary purpose of this article is to consider the powers available to the ACCC to investigate potentially problematic algorithms, it is vital that regulated entities are aware of their obligations and comply with any current or future regulatory regime. This Part summarises regulatory theory and highlights recent compliance experience relevant to achieving these ends.

Harrington has highlighted the importance of ensuring that liability is clearly defined, positing that '[i]f managers do not know when they are acting unlawfully then illegal behaviour cannot be deterred'.[123]

Under his proposed model of per se liability as discussed above,

> managers would be able to determine when they are in compliance with the law by having the learning algorithm programmed to engage in periodic testing of the pricing algorithm to ensure it does not exhibit the prohibited property.[124]

Murphy et al find that 'attitudes and moral obligations, in addition to economic calculations or fear of punishment, are important in explaining compliance behaviour'.[125]

This is supported by Braithwaite, who noted that appealing to the moral codes of business leaders is likely to be more successful than deterrence.[126] Ohm has optimistically suggested that certain firms be obligated to be 'forthright' in their dealings with consumers.[127]

---

120 Ibid.

121 Ibid.

122 See Rob White and Santina Perrone, *Crime, Criminality & Criminal Justice* (Oxford University Press, 1st ed, 2010) 53.

123 Harrington (n 77) 356.

124 Ibid.

125 Kristina Murphy, Tom R Tyler and Amy Curtis, 'Nurturing Regulatory Compliance: Is Procedural Justice Effective When People Question the Legitimacy of the Law?' (2009) 3(1) *Regulation and Governance* 1, 2 (citations omitted).

126 John Braithwaite, *Restorative Justice and Responsive Regulation* (Oxford University Press, 2001) 33.

127 Paul Ohm, 'Forthright Code' (2018) 56(2) *Houston Law Review* 471, 485–6.

Additionally, Murphy et al make clear that it is vital that any regulation undertaken by use of legal authority must not be considered by those regulated to be 'unreasonable' in order for it to have the greatest chance of achieving compliance.[128] Cooperative enforcement has been found to increase compliance, whilst 'persuasion and fair treatment of regulatees during regulatory encounters' by maintaining procedural justice is similarly hypothesised to increase compliance because it increases the 'perceived legitimacy' of a regulatory authority.[129]

The Hon Kenneth Hayne AC QC has considered the economic motivations of compliance, on the implicit assumption that corporate actors are rational, highlighting his view that regulators must ensure that breaches of the law are 'not profitable'.[130] The optimal deterrence theory holds the probability of detection as a key variable in the calculus of determining compliance.[131] Under the algorithmic scrutiny power proposed below in this article, the probability of detecting concerning algorithmic conduct may increase. If supported by relevant liability laws and penalties, under this view, this proposal may increase compliance.

However, the classical view presupposes that humans are only rational actors that undertake an 'expected utility' decision by weighing up their likelihood of detection, potential penalties, and potential profits to be gained from a contravention in determining whether or not to break the law.[132] This approach was initially promulgated by Beccaria, and later developed by Bentham.[133] The approach has been the subject of considerable debate as to its effectiveness.[134] As mentioned above, the classical approach is countered by Braithwaite[135] and Murphy et al[136] who find that individual morals may be a greater determinant of compliance. Braithwaite has noted that increasingly punitive corporate sanctions may lead a company to organise its reporting structure such that it may be 'counter-deterred' by reporting lines that seek to abrogate the responsibility of a top-down non-compliance direction or non-compliant culture from Chief Executive Officer, to Vice Presidents 'responsible for going to jail'.[137]

The classical approach is challenged by what academics have labelled the 'deterrence gap' or 'deterrence trap'. The 'deterrence trap' exists by virtue of corporate structures and their inter-dependence with stakeholders such as employees that there is a limit of the quantum of a deterrent penalty that can be imposed without it having negative side effects on wider corporate stakeholders.[138] For example, precipitating corporate financial hardship that leads to employee

128 Murphy, Tyler and Curtis (n 125) 2.
129 Ibid.
130 *Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry* (Final Report, 1 February 2019) vol 1, 427.
131 A Mitchell Polinsky and Steven Shavell, 'The Economic Theory of Public Enforcement of Law' (2000) 38(1) *Journal of Economic Literature* 45, 47–8; Gary Becker, 'Crime and Punishment: An Economic Approach' (1968) 76(2) *Journal of Political Economy* 169, 176.
132 Polinsky and Shavell (n 131) 47. An example is provided by Braithwaite (n 126) 108.
133 White and Perrone (n 122) 53–5.
134 Braithwaite (n 126) 102.
135 Ibid 33.
136 Murphy, Tyler and Curtis (n 125) 2.
137 Braithwaite (n 126) 108.
138 Ibid.

layoffs and destruction of (arguably innocent) shareholder value. Contrastingly, the 'deterrence gap' explains that by targeting a company with sanctions, the actors responsible within that company are shielded by the corporate structure and therefore do not receive the just deserts for their misconduct.[139]

Sutherland's theory of 'differential association' can explain cultures of corporate compliance or non-compliance, where peer interactions shape individual attitudes about whether to comply with legal and regulatory obligations.[140] This can be compared to Feldman's book in the emerging field of 'behavioural ethics'[141] where he found that while harsh sanctions may 'deter calculative people',[142] they may do the opposite for 'situational wrongdoers'[143] and genuinely moral yet 'erroneous wrongdoers'[144] 'who engage in noncompliance with limited awareness'.[145]

However, recent experience in the UK, as well as the Australian Financial Services Royal Commission appears to highlight that deterrent penalties still play an important role in disincentivising non-compliance. For example, the supply chain reporting obligation under the *Modern Slavery Act 2005* (UK) currently lacks penalties and other enforcement remedies other than the ability for the Secretary of State to seek a mandatory injunction.[146]

This has been recognised as a key factor contributing to its widespread non-compliance.[147] It has been estimated that as few as 60% of businesses required to comply with that obligation do so.[148] This figure is as low as 19% in the agricultural sector.[149]

---

139 Simon Bronitt and Alessia D'Amico, 'Fighting Cartels and Corporate Corruption – Public Versus Private Enforcement Models: A False Dichotomy?' (2018) 37(1) *University of Queensland Law Journal* 69, 75.

140 Robert Apel and Raymond Paternoster, 'Understanding "Criminogenic" Corporate Culture: What White-Collar Crime Researchers Can Learn from Studies of the Adolescent Employment–Crime Relationship' in Sally S Simpson and David Weisburd (eds), *The Criminology of White-Collar Crime* (Springer, 2009) 15, 15–19 <https://doi.org/10.1007/978-0-387-09502-8_2>.

141 Yuval Feldman, *The Law of Good People: Challenging States' Ability to Regulate Human Behavior* (Cambridge University Press, 2018) 2–5.

142 Ibid 154.

143 Ibid 61.

144 Ibid.

145 Ibid 154.

146 *Modern Slavery Act 2005* (UK) s 54(11).

147 Secretary of State for the Home Department, *Independent Review of the Modern Slavery Act 2015: Final Report* (CP 100, 2019) 39 [1.4] <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/803406/Independent_review_of_the_Modern_Slavery_Act_-_final_report.pdf>.

148 Home Office (UK), 'Home Office Tells Business: Open up on Modern Slavery or Face Further Action' (News Story, 18 October 2018) <https://www.gov.uk/government/news/home-office-tells-business-open-up-on-modern-slavery-or-face-further-action>.

149 Andrew Phillips and Alexander Trautrims, 'Agriculture and Modern Slavery Act Reporting: Poor Performance Despite High Risks' (Research Report, Office of the Independent Anti-Slavery Commissioner and the University of Nottingham's Rights Lab, 15 August 2018) 4 <http://www.antislaverycommissioner.co.uk/media/1220/modern-slavery-act-and-agriculture-poor-performance-briefing.pdf>.

Whilst recognising that the law typically follows behind technological innovation,[150] Leenes et al advocate for 'responsible research and innovation', which is

> a transparent, interactive process by which societal actors and innovators become mutually responsive to each other with a view on the (ethical) acceptability, sustainability and societal desirability of the innovation process and its marketable products …[151]

A type of 'regulatory ambassador', as proposed by Braithwaite and Hong,[152] may act as the interface between a regulated entity and the regulator. This is likely to facilitate better regulatory experiences by both parties, especially within the unsettled and adaptive world of technological regulation. The ambassador should be responsible for advocating for 'compliance-by-design' programming within their organisation.[153] Fosch-Villaronga and Heldeweg have also proposed an iterative model of regulation in relation to artificial intelligence more broadly.[154]

Officers and employees of corporations must be responsible for programming compliant algorithms. Programmers and their chain of management should have a direct and vicarious responsibility to ensure appropriate safeguards and limitations are present in their algorithms. In the case of self-learning algorithms, the failure to enable 'safe interruptibility'[155] should not be a defence to the programming or operation of an anti-competitive or misleading algorithm.[156] Because of the identified importance of detection of potential contraventions of the law in order to maximise deterrence, the ACCC must have appropriate information gathering capabilities that are suitable for use in technology-driven market contexts.

V EVALUATION OF THE ACCC'S INFORMATION GATHERING POWERS UNDER SECTION 155 OF THE *CCA*

This Part considers the primary legal avenue through which the ACCC is empowered to seek documents, information, and oral evidence. This Part finds that while the powers are broad, they are not sufficiently fit for the purpose of proactive investigation and monitoring of potentially harmful algorithms.

---

150 Ronald Leenes et al, 'Regulatory Challenges of Robotics: Some Guidelines for Addressing Legal and Ethical Issues' (2017) 9(1) *Law, Innovation and Technology* 1, 35.

151 René von Schomberg, 'Introduction' in René von Schomberg (ed), *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Field* (European Commission, 2011) 7, 9.

152 John Braithwaite and Seung-Hun Hong, 'The Iteration Deficit in Responsive Regulation: Are Regulatory Ambassadors an Answer?' (2015) 9(1) *Regulation and Governance* 16.

153 Colombo (n 76) 20.

154 Eduard Fosch-Villaronga and Michiel Heldeweg, '"Regulation, I Presume?" Said the Robot – Towards an Iterative Regulatory Process for Robot Governance' (2018) 34(6) *Computer Law and Security Review* 1258.

155 See Laurent Orseau and Stuart Armstrong, 'Safely Interruptible Agents' (Research Paper, Machine Intelligence Research Institute, 28 October 2016) <https://intelligence.org/files/Interruptibility.pdf>.

156 Colombo (n 76) 20.

A Background to the Powers

CCA section 155(1) provides the ACCC with the 'powerful investigative tool'[157] of being able compel a person, by notice, to provide information,[158] documents,[159] or attend an examination.[160] A notice may be issued by the Commission, Chair, or Deputy Chair of the ACCC. This article does not comprehensively assess the section 155 powers in a broad context but focuses on their relevance to the topic of this article. Wylie comprehensively examined the ACCC's evidence-gathering powers in 2009,[161] but further evaluation is overdue.

The ACCC issued 236 such notices in 2017–18.[162] In that period, none were subject to legal challenge.[163]

B Statutory Interpretation of Section 155

Exercising this power requires that the issuer has a 'reason to believe'[164] that a person is capable of giving evidence relating to a 'matter'[165] that 'constitutes or may constitute a contravention' of the *CCA*, *Australian Consumer Law*, an enforceable undertaking,[166] or is otherwise relevant to a number of other enumerated matters.[167] For example, these enumerated matters include an inquiry into the terms of a 'consumer contract or small business contract'.[168]

The approach to constructing section 155(1) is well established. Re-stating the approach to construction as summarised by Sackville and Emmett JJ in *Seven Network Ltd v Australian Competition and Consumer Commission* ('*Seven Network*'),[169] the Court in *Singapore Airlines v Australian Competition and Consumer Commission* ('*Singapore Airlines*') highlighted that

> in order to satisfy the requirements of s 155(1), it must appear from the terms of the notice that it seeks information 'relating to a matter' of a kind described in that subsection … In determining that question, the court is not to adopt a 'precious', 'over-technical' or 'hypercritical' approach to the construction of the notice … the word 'matter' is to be construed in its ordinary sense …[170]

While it is clear that the courts take a permissive approach to the interpretation of notices under section 155(1), a notice under section 155(1) may only be issued

---

157 *SA Brewing Holdings Ltd v Baxt* (1989) 23 FCR 357, 359 (Fisher and French JJ).
158 *CCA 2010* (Cth) s 155(1)(a).
159 Ibid s 155(1)(b).
160 Ibid s 155(1)(c).
161 Ian Wylie, 'When Too Much Power Is Barely Enough: s 155 of the *Trade Practices Act* and Noblesse Oblige' (2009) 16(3) *Competition and Consumer Law Journal* 314.
162 Australian Competition and Consumer Commission and Australian Energy Regulator, *Annual Report 2017–18* (Report, October 2018) 298.
163 Ibid.
164 *CCA 2010* (Cth) s 155(1).
165 Ibid.
166 Ibid s 155(2)(a).
167 Ibid s 155(2)(b).
168 Ibid s 155(2)(b)(v).
169 (2004) 140 FCR 170, 182 [49] ('*Seven Network*').
170 (2009) 260 ALR 244, 250 [35]–[38] (Black CJ, Mansfield and Jacobson JJ) (citations omitted) ('*Singapore Airlines*').

in circumstances where there is as 'matter'[171] and the decision maker has formed a 'reason to believe' that the addressee is capable of furnishing evidence in relation to that 'matter'.[172]

C Section 155 Is Not Fit for Proactive Purposes

The section 155 powers have proven themselves to be generally industry and technology non-specific, with the *Seven Network* and *Singapore Airlines* cases concerning matters in the offline world. However, it is argued that the proposals detailed in Part VI of this article are better adapted to gathering information and determining consumer harm in a digital world, especially where a contravention of the *CCA* may not have yet materialised.

This necessarily means that notices where the 'matter' is a 'contravention'[173] are reactive rather than proactive. This is because the issuer must have apprehended the possible existence of facts that may, if found, have given rise to a contravention of the *CCA*.[174] Thus, section 155(1) notices are not suitable for proactive information gathering that aims to address potential harms to competition prior to them potentially materialising into contraventions of the *CCA*. Section 155(1) can only be used proactively, when the 'matter' is 'relevant to' one of the matters enumerated under *CCA* section 155(2)(b).

Section 155 does not contemplate nor require the establishment of a specified technical data request and response protocol for the respondent to provide requested information. Further, section 155 does not expressly contemplate nor provide for the observation nor the carrying out of simulations or experiments on any algorithms under the control of the respondent.

Given the limitations of the section 155 power to proactively monitor and test the effects of algorithms, this article now proposes two new technical measures for algorithm monitoring by the ACCC and data transfer to the ACCC, in order to increase the possibility of detection of contraventions of the *CCA* and *Australian Consumer Law*.

VI APPLICATION PROGRAMMING INTERFACE PROPOSALS

A Outline of Proposals

This Part proposes the establishment of a standardised regulatory application programming interface ('API') to enable two key investigatory powers. First, an 'algorithm scrutiny power' that enables the ACCC to undertake experiments on key algorithms of monitored firms, whether or not they are public-facing.

Second, this Part proposes a 'data request power' that enables the ACCC to access commercial data of monitored firms in order to support the proactive monitoring of potential competition issues, including cartel detection and

171 *CCA 2010* (Cth) s 155(2)(a)(i).
172 *Seven Network* (2004) 140 FCR 170, 182 [49](iii) (Sackville and Emmett JJ).
173 *CCA 2010* (Cth) s 155(2)(a).
174 *Singapore Airlines* (2009) 260 ALR 244, 250 [37] (Black CJ, Mansfield and Jacobson JJ).

concerted practices. This article does not directly articulate a case necessarily requiring the imposition of this second power.

In relation to the proposed data request power, it is noted that the *DPI Final Report* did not appear to contemplate a broad bulk data gathering power,[175] but envisaged high-level summary information in a similar form and to what is provided by energy retailers to the Australian Energy Regulator.[176] Further, it is noted that when ACCC Chair Rod Sims suggested 'throwing a lot of things at [Facebook's and Google's] algorithms,'[177] it is uncertain whether he implied that this be undertaken through a novel investigative process. Rather, having a staff member undertake specific experiments or observations through usual interfaces, such as a web browser or mobile apps, may have been in contemplation.

While it would be challenging, both powers should ideally be developed as international or industry standards in order to reduce the regulatory burden on firms operating transnationally; if the same or similar powers are adopted by regulators in jurisdictions other than Australia. However, the Australian context is the primary focus of this article. The technical protocols contemplated in the below proposals should implement ubiquitous digital standards, such as 'Representational State Transfer'[178] and should build on the capability developed by the ACCC and Data61 in developing and implementing regulated technical standards through the Consumer Data Right.[179]

B How Should the Powers Be Exercised?

Both powers could be exercised on an ad-hoc per-notice basis, or as part of an ongoing monitoring protocol as agreed between the regulator and the monitored firm, or as required by law, perhaps through the use of a standing notice.

The responsibility of the below two powers may primarily be exercised by the ACCC's new Digital Platforms Branch, as the capability of that branch in relation to technology and novel, primarily digital-based, competition and consumer concerns most closely aligns with this proposal. However, the administration of these powers may risk distracting the Digital Platforms Branch from its initial and primary mandate of monitoring digital platforms,[180] as opposed to potentially

175 *DPI Final Report* (n 1) 140–1.

176 See Australian Energy Regulator, *AER (Retail Law) Performance Reporting Procedures and Guidelines* (Performance Report, April 2018) <https://www.aer.gov.au/system/files/AER%20Retail%20Law%20Performance%20Reporting%20Procedures%20and%20Guidelines%20-%20January%202019%20%E2%80%93%20from%20Q3%202018-19.pdf>; *DPI Final Report* (n 1) 141.

177 ACCCgovau (Australian Competition and Consumer Commission), 'ACCC Digital Platforms Inquiry' (n 4) 00:16:33–00:16:38.

178 See Roy Thomas Fielding, 'Architectural Styles and the Design of Network-Based Software Architectures' (Dissertation, University of California, 2000) ch 5 <https://www.ics.uci.edu/~fielding/pubs/dissertation/fielding_dissertation.pdf>; Martin Fowler, 'Richardson Maturity Model', *martinFowler.com* (Web Page, 18 March 2010) <https://martinfowler.com/articles/richardsonMaturityModel.html>.

179 See generally Data61, 'Standards', *Consumer Data Standards* (Web Page, 30 September 2019) <https://consumerdatastandardsaustralia.github.io/standards/#standards>.

180 Australian Competition and Consumer Commission, 'Holistic, Dynamic Reforms Needed to Address Dominance of Digital Platforms' (Media Release No 124/19, 26 July 2019)

competition-affecting algorithms in general. It is expected that there will be significant ongoing collaboration with the Digital Platforms Branch and the ACCC's Strategic Data Analysis Unit in order to determine what datapoints are required,[181] establish data management processes and workflows, and in interpreting the results of data gathering.

These powers may be considered too interventionist in an environment where there has been no proven cases of colluding algorithms and the exact consumer harms remain to be seen. Nonetheless, the proposed powers put forward in this article provides a discussion point for regulators and policymakers to consider how their liability rules, investigative practices and procedures can or should adapt to the challenges posed by new technology. The proposals also raise privacy, data security and regulatory creep concerns, which while not insurmountable, must be overcome or appropriately mitigated.

The following sub-Part outlines each of the two proposed powers.

C Algorithm Scrutiny Power

1 What Is the Proposal?

In addition to such algorithm scrutiny that may be performed by an ACCC officer accessing a website or other public interface, this algorithm scrutiny power seeks to establish a uniform technological protocol between the ACCC and monitored firms in order to provide the ACCC with the capacity to test algorithms for competitive or consumer harm. Under this power, a uniform request and response protocol is created, allowing the ACCC to send a request to a monitored firm, including relevant inputs, to a particular algorithm of the firm, and receive a response in a standardised format.

This is likely to require collaboration between each monitored firm and the ACCC in order to implement the protocol. Alternatively, a requirement may be imposed where each algorithm that meets certain potentially 'high risk' properties must conform to the API standards to allow a regulator to more simply monitor it. It is possible that a sandboxed replica of the actual live algorithm may be used to run the targeted algorithm under the API request from the ACCC. Additionally, there must be consideration of access permissions, privacy, and data security. Similar to the data request power description below, once the ACCC receives the response, it may be saved for later analysis, or automatically be entered into an existing data analysis workflow.

<https://www.accc.gov.au/media-release/holistic-dynamic-reforms-needed-to-address-dominance-of-digital-platforms>.

181 Rod Sims, 'The ACCC's Approach to Colluding Robots' (Speech, Can Robots Collude? Conference, 16 November 2017) s 2 <https://www.accc.gov.au/speech/the-accc%E2%80%99s-approach-to-colluding-robots>.

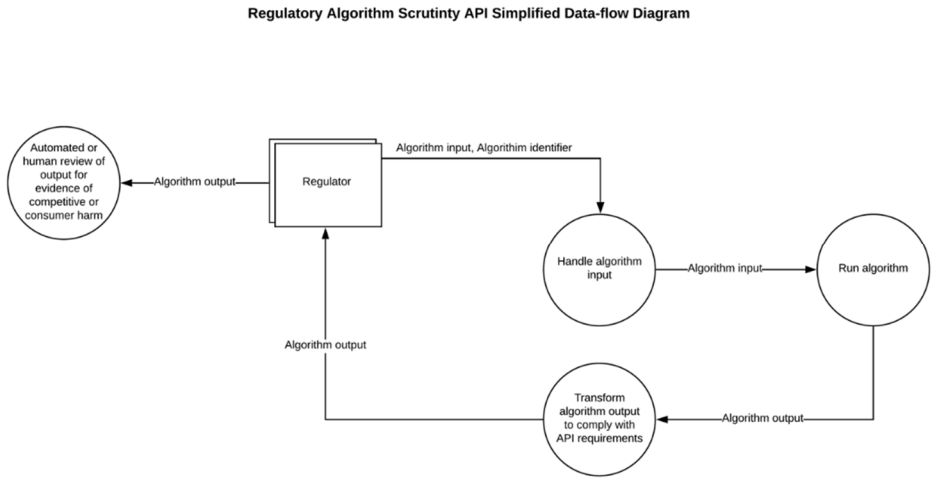

Figure 1: Abstract data-flow diagram illustrating the flow of data between the regulated entity and the regulator under the proposed algorithm scrutiny power.

2 What Types of Algorithms Does the Proposal Apply to?

In relation to potential horizontal collusion, analysis should seek to discover algorithms that may exhibit anti-competitive properties that attempt to or actually influence the response of competitors, including:

'one-period punishment' algorithms;[182]

'tit for tat' algorithms;[183] and

'permanent reversion to competition [punishment]' algorithms.[184]

In relation to vertical competition, algorithms that may seek to monitor or enforce resale price maintenance should also be the subject of analysis.[185]

In relation to other algorithms of competitive or consumer concern, analysis should seek to discover algorithms that may, for example:

self-preference;[186] or

demote the position of certain suppliers, based on their refusal to comply with a potentially anti-competitive stipulation.[187]

182 Harrington (n 77) 345.

183 Ibid.

184 Ibid.

185 See European Commission (n 20); Nicholls (n 6).

186 Nicolo Zingales, 'Google Shopping: Beware of "Self-Favouring" in a World of Algorithmic Nudging', *Competition Policy International* (Web Page, 13 February 2018) <https://dev.competitionpolicyinternational.com/google-shopping-beware-of-self-favouring-in-a-world-of-algorithmic-nudging/>; Jacques Crémer, Yves-Alexandre de Montjoye and Heike Schweitzer, *Competition Policy for the Digital Era* (Final Report, 4 April 2019) 7, 66–8 <https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf>.

187 See, eg, Elmas (n 44); Australian Competition and Consumer Commission, 'Expedia and Booking.Com Agree to Reinvigorate Price Competition by Amending Contracts with Australian Hotels' (Media Release

The proposal may also see future application against other opaque algorithms. For example, the ACCC has opined that the opacity of Facebook and Google's advertising algorithms may not be appropriate in order to ensure that advertisers are 'informed of the outcomes'.[188]

D Data Request Power

1 What Is the Proposal?

The data request power seeks to establish a uniform technological protocol for the request and transfer of data from a 'monitored firm' and the ACCC. A 'monitored firm' may include a company supplying or receiving goods or services, including government and private organisations that undertake a tendering process. Under this power, the ACCC would have an interface to make a request for specific data. That request would then be sent to the receiving monitored firm, specifying the data sought. The data sought would be of a kind or category that is pre-set as part of the API protocol. Upon receiving the data request, the monitored firm's system would recognise the data sought and retrieve the data from the relevant data store. Then, it is expected that the system would perform any intermediate steps, including transforming the data into an appropriate format for the API, before sending it back to the ACCC. Upon receiving the response, the ACCC would then suitably store the data for later analysis, or 'pipe' the data into an existing data analysis workflow.

2 To What Does the Proposal Apply?

While this article does not directly articulate the case for the imposition of this power, it is the author's view that it is technologically expedient to consider future applications of regulatory APIs in order to ensure the implementation of a flexible and adaptable protocol. This has the goal of minimising the long-term burden on regulated entities and the regulator when using similar technology in regulation into the future.

The section 155 powers have begun to acknowledge the digital era. This is manifested through the requirement that a person is not required to perform more than a 'reasonable search' for documents.[189] The 'reasonable search' defence was introduced to reduce the burden of complying with notices following a recommendation by the *Harper Review* because of the large amounts of documents being generated within computer-driven organisations.[190] The defence is not mirrored under section 95ZK of the *CCA*, with its closest comparable defence being the 'reasonable excuse'[191] defence – which is not available under section 155.[192] Section 95ZK of the *CCA* is otherwise very similar to section 155, but is

No 158/16, 2 September 2016) <https://www.accc.gov.au/media-release/expedia-and-bookingcom-agree-to-reinvigorate-price-competition-by-amending-contracts-with-australian-hotels>.

188 *DPI Final Report* (n 1) 12.

189 *CCA 2010* (Cth) s 155(5B)(b).

190 Ian Harper et al, *Competition Policy Review* (Final Report, 31 March 2015) 71.

191 *CCA 2010* (Cth) s 95ZK(5).

192 Ibid s 155(7).

limited to information gathering in ministerially directed or approved 'inquiry' contexts.[193]

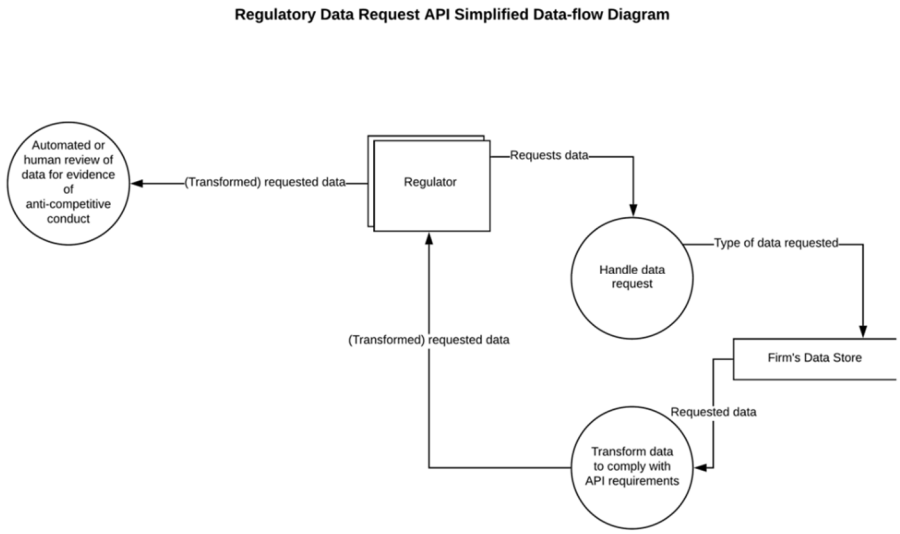

Figure 2: Abstract data-flow diagram illustrating the flow of data between the regulated entity and the regulator under the proposed data request power.

E Proposed Powers in Practice and Law

The proposals in this article require consideration of their practical and legal implications.

First, the powers ought to add to consideration of the capability of the ACCC and competition regulators in considering how they will respond to increasingly challenging technological environment that may exceed their current investigatory toolkit. Second, consideration must be given to how the legal framework supports or may have to change in order to support a unique investigatory environment of the future.

The investigatory powers of the ACCC do not exist in a vacuum. The ACCC receives most of its information voluntarily.[194] However, the legal backing under section 155 to compulsorily acquire information adds to the legitimacy of ACCC information (including document) gathering, and encourages co-operation in order to incentivise the targets of information requests to provide information or documents voluntarily as opposed to having to be compelled by notice to comply. As foregrounded in Part V, the powers under section 155 are only enlivened when

193 Ibid pt VIIA.

194 Australian Competition and Consumer Commission, 'ACCC Guidelines: Use of Section 155 Powers' (Guideline, June 2020) 2 <https://www.accc.gov.au/system/files/1582RPT_ACCC%20Guidelines-Use%20of%20section%20155%20powers_FAJune20.pdf>.

the issuing decision maker forms a 'reason to believe'[195] that the addressee is capable of providing evidence relating to a 'matter'[196] that 'constitutes or may constitute a contravention',[197] or is relevant to a number of other enumerated matters,[198] including an inquiry into the terms of a 'consumer contract or small business contract'.[199]

1 Compulsory Production of Information

It is unlikely that the mere use of an algorithm in the ordinary course of business, in the absence of a complaint or any other evidence to support the suspicion of a contravention of the *CCA*, for example under the prohibition on concerted practices,[200] would satisfy the general 'matter' requirement of section 155(1). As mentioned above in Part V, this means that notices under this limb may only be issued reactively. However, there are two potential alternative methods for enlivening compulsory information gathering powers, especially in relation to the algorithm scrutiny power as proposed in this article.

The first is to enumerate and append a relevant matter in terms of or similar to 'the Commission investigating or inquiring into the use of an algorithm' to the list of matters under section 155(2)(b). The alternative is that an inquiry under *CCA* part VIIA is undertaken under terms of reference that would enable the compulsion of relevant information under section 95ZK.[201] On 10 February 2020, the ACCC was directed to undertake such an inquiry; but limited to inquiring into 'the markets for the supply of digital platform services'.[202] Section 95ZK of the *CCA* is similar in form and effect to section 155, but provides for the compulsion of documents, information and oral evidence 'relevant to' an inquiry held under part VIIA.[203] Non-compliance with a notice on the basis of self-incrimination is not generally permitted under a section 155 notice,[204] but is a defence to non-compliance under a section 95ZK notice.[205]

2 Form and Protocol

Whilst both sections 155 and 95ZK of the *CCA* provide for the compulsion of information, documents, and oral evidence, they do not prescribe the form or manner in which such information or documents are to be provided. Further, they do not directly authorise the testing or auditing of systems, nor the direct experimentation with systems by the ACCC.

The inability to prescribe the form and manner of a response means that the algorithm scrutiny power and data request power of this article goes beyond what

195 *CCA 2010* (Cth) s 155(1).
196 Ibid.
197 Ibid s 155(2)(a).
198 Ibid s 155(2)(b).
199 Ibid s 155(2)(b)(v).
200 Ibid s 45(1)(c).
201 See ibid s 95H.
202 *Competition and Consumer (Price Inquiry–Digital Platforms) Direction 2020* (Cth) cl 5(1).
203 *CCA 2010* (Cth) s 95ZK(1).
204 Ibid s 155(7).
205 Ibid ss 95ZK(4)–(6).

is now legally required of firms in order to comply with a notice made under either of those two information gathering provisions. Sections 155 and 95ZK of the *CCA* can be contrasted against the compliance and performance reporting requirements of the *National Energy Retail Law*[206] where the Australian Energy Regulator ('AER') prescribes the manner and form of the information to be received under the 'AER Compliance Procedures and Guidelines'[207] and the 'AER Performance Reporting Procedure and Guidelines'.[208]

While the *National Energy Retail Law* does not provide a directly analogous example, as it concerns information periodically provided to the AER, as opposed to on an ongoing basis or through an access protocol, it nonetheless demonstrates an industry-wide precedent for specifically prescribed methods of regulatory reporting.

A similar scheme exists in the telecommunications industry, where the ACCC can make 'record keeping rules' and require regulated entities to prepare and provide to it reports based on those kept records.[209] However, there appears to be voluntary discussion between the ACCC and firms subject to a section 155(1)(b) notice as to the methodology of electronically producing documents.[210]

Consideration should also take place about whether a power for the ACCC to be able to conduct 'experiments' on systems under a section 155 or section 95ZK notice, in addition to being able to compel information and documents should be implemented.

Coming to an exact proposal for a technological, legal and practical protocol under which the algorithm scrutiny and data request powers can be exercised will require substantial consultation and consideration from stakeholders including industry, technology experts, software developers, and regulators.

A recent area where this type of consultation has been performed in order to mandate technological requirements on firms is with the Consumer Data Right.[211] In that case, numerous agencies consulted on different aspects of the regime. As stated in the Government's response to the *Review into Open Banking*,[212] 'Treasury will be consulting on draft legislation, the ACCC will be consulting on draft rules, and Data61 will be consulting on technical standards'.[213]

An alternative approach may be for the ACCC to engage with a limited number of firms that have implemented or are currently implementing pricing or other types of algorithms that may be viewed as competitively risky. Through this

206 *National Energy Retail Law (South Australia) Act 2011* (SA) ss 274, 282.

207 Ibid s 281.

208 Ibid s 286.

209 *CCA 2010* (Cth) s 151BU.

210 Australian Competition and Consumer Commission, 'ACCC Guidelines: Use of Section 155 Powers' (n 194) 10.

211 'Treasury Laws Amendment (Consumer Data Right) 2018 Bill', *Australian Government* (Web Page, 2018) <https://webarchive.nla.gov.au/awa/20190327094421/http://www.treasury.gov.au/consumer-data-right-bill>.

212 Scott Farrell, Treasury, *Review into Open Banking: Giving Customers Choice, Convenience and Confidence* (Report, December 2017) <https://treasury.gov.au/sites/default/files/2019-03/Review-into-Open-Banking-_For-web-1.pdf>.

213 'Government Response to Review into Open Banking', *Australian Government* (Web Page, 9 May 2018) <https://treasury.gov.au/publication/p2018-t286983>.

collaboration, an iterative approach can be adopted to the practical design and implementation of the algorithm scrutiny and data request powers. This can take the form of a pilot. If successful, a broader consultation should follow prior to the potential imposition of this intervention on more firms, in cases justified by a threat of competitive or consumer harm.

If not legislated or a voluntary arrangement is not forthcoming, the ACCC may consider the algorithm scrutiny and/or data request power as an obligation that can be imposed through a remedy with each specific firm. For example, as an undertaking under section 87B of the *CCA* as part of a conditional merger approval or investigation resolution.

A stop-gap solution for the auditing of algorithms may be to have firms self-assess particular capabilities of their algorithms by performing specified tasks and reporting their results back to the ACCC under a *CCA* section 155(1)(a) or a section 95ZK(1)(e) information request. In *Seven Network*, Tamberlin J held that the term 'information' should be given its ordinary 'broad and far-reaching' meaning.[214] This means that it may be possible for an information request to ask an officer of a company to do a certain thing with its algorithm and report back their result. However, the extent to which an information request can be used requiring positive action will be limited. It is likely that the 'thing' that can be asked of a person must be 'read only' and not otherwise affect the operation or state of a system. The extent and ability of sections 155 and 95ZK to cover these types of matters could be clarified by legislative amendment.

3 Risks, Challenges, and Alternatives

The two proposals detailed in this article are not without their challenges. These include increasing the regulatory burden on firms, the difficulty and time required to establish transnational standards, as well as potential concerns of regulatory overreach. In addition, if firms are to engage with either power, they will have concerns over data protection, privacy, and confidentiality. It is important for the protection of personal or confidential information that 'backdoors'[215] which could introduce information security vulnerabilities are not created. Similarly, the storage of personal information which could be captured under the proposed powers, could be vulnerable to attack should be avoided or, at the very least, strongly protected. This will require that any new regulatory powers are appropriately defined, restricted and reviewed in their usage. Additionally, there is a risk to the regulator that firms may seek to mislead or 'greyball' regulatory investigations or enforcement efforts by providing access to fake algorithms that may minimise the potential competitive or consumer harms.[216] While this article raises an initial proposal, additional consideration and exploration of these challenges and methods to address them are warranted. This

214 *Seven Network* (2004) 140 FCR 170, 175–6 [18].

215 Kim Zetter, 'Hacker Lexicon: What Is a Backdoor?', *Wired* (Web Page, 11 December 2014) <https://www.wired.com/2014/12/hacker-lexicon-backdoor/>.

216 See Mike Isaac, 'How Uber Deceives the Authorities Worldwide', *The New York Times* (online, 3 March 2017) <https://www.nytimes.com/2017/03/03/technology/uber-greyball-program-evade-authorities.html>.

will require public consultation, including input by firms potentially captured by the proposals.

Less invasive alternatives to the imposition of the powers proposed in this article may achieve similar outcomes with a lower regulatory burden. For example, instead of the 'algorithm scrutiny power' as described above, entities may devise an industry standard or code to mitigate against collusive or misleading algorithms. Compliance could be self-verified, verified by the ACCC, or by a third-party auditor. Similarly, instead of the 'data request power' being imposed on supply firms in a market, the ACCC could, for example, seek and analyse procurement data from customers. This is performed in South Korea, where the competition regulator analyses and screens for signs of bid rigging the procurement information of public tenderers.[217] In the UK, the Competition and Markets Authority provide software to assist procurement personnel in identifying indicators of bid rigging.[218] There is no regulatory panacea, but thoughtful consideration of potential harms and responses can seek to maximise overall consumer welfare whilst minimising the introduction of new risks, unduly increasing the regulatory burden on firms, or substantially reducing innovation.

VII CONCLUSION

The digital era presents a multitude of economic opportunities, as well as corresponding risks. This article explored four categories of potential consumer harm that may arise through the usage of algorithms. The categories are (i) algorithms that may assist in creating or enforcing vertical or horizontal restraints; (ii) algorithms that enable self-preferencing by dominant platforms; (iii) algorithms that may facilitate the enforcement of anti-competitive contractual restrictions; and (iv) ranking algorithms that may mislead consumers.

This article particularly focused on the potential of algorithms to tacitly horizontally collude. While in this case the exact harms remain unknown, algorithmic practices by firms have been experiencing increased scrutiny by regulators, policymakers, and academics worldwide. To respond to potential contraventions of the law, regulatory theories may be invoked on the assumption that applying them will deter such contraventions from materialising.

This article found that the general consensus is that general deterrence of breaches of the law results from the threat of detection and the potential for large penalties in response. However, there is emerging behavioural literature to suggest that strong sanctions may not prevent contraventions of the law by people who are

---

217 'Country Case: Korea's Bid Rigging Indicator Analysis System (BRIAS)', *Organisation for Economic Co-operation and Development* (Web Page, 2016) <https://www.oecd.org/governance/procurement/toolbox/search/korea-bid-rigging-indicator-analysis-system-brias.pdf>.

218 Competition and Markets Authority, 'CMA Launches Digital Tool to Fight Bid-Rigging' (Press Release, UK Government, 15 December 2017) <https://www.gov.uk/government/news/cma-launches-digital-tool-to-fight-bid-rigging>.

not calculated and intentional contraveners.[219] Additionally, new models such as 'regulatory ambassadors'[220] have been suggested, but their efficacy remains untested. Given the importance of detection of potential contraventions to deterrence-based theories, the ACCC's statutory information and document gathering powers under sections 155 and 95ZK of the *CCA* are analysed from the perspective of them being used to proactively monitor algorithms. The article finds that they are, in their current form, unable to be used for proactive monitoring purposes in most cases. Additionally, the legislation does not expressly provide for an ability for the ACCC to be able to perform experiments nor test the functionality of systems or algorithms. Because of the drawbacks of the information gathering powers in their current form, the article then argues for a standardised regulatory API through which an 'algorithm scrutiny power' and 'data request power' can operate. It is argued that this additional technological and legal capability is required for the ACCC to most effectively interrogate the potential harms of algorithms, whilst providing a mechanism for future enforcement and compliance work. The article considers how and when the powers could be exercised, as well as consideration of some of the challenges and risks associated with them. Less burdensome industry-led alternatives are also suggested.

This article has established a legal and technical starting point from which regulators, policymakers and academics can consider regulatory information gathering practice and procedure that maximise consumer welfare and protection in the age of algorithms.

219 Feldman (n 141).
220 Braithwaite and Hong (n 152).