<u>Abstract (300 words)</u>

I start with the thesis that artificial intelligence ("AI") is morally neutral. AI's development should be shaped in a pro-social direction, and there is no inherent conflict between protecting competition and consumers and advancing technology.

I observe that AI can facilitate common existing types of competition and consumer law violations. These are easy cases as such situations can be governed by existing laws.

I then tackle the harder issue of *new* problems created by AI, including the unpredictability of AI collusion due to opacity of machine learning algorithms and the rapid pace of AI advancements. I suggest that regulatory insights can be gleaned from adjacent fields. Useful ideas to consider include the concept of "enterprise risk" and elements from the law on vicarious liability and attribution.

I recommend that the Competition and Consumer Commission of Singapore ("CCCS") tap on its extensive powers to require production of information by companies. By examining AI source code and usage logs, regulators can form a view as to whether AI tools have been used in a manner that infringes competition and consumer law. Regulators should encourage candid and proactive disclosures, and be ready to engage in constructive dialogue when companies apply for guidance or decisions. Such dialogues offer a chance for regulators to gain access – upstream – to information about latest AI developments and to help shape future AI development.

I note that AI tools help regulators with enforcement by churning through large volumes of data quickly and intelligently.

I also note that AI, coupled with big data, can allow regulators and consumer associations to promote transparency which in turn promotes consumer choice. I

suggest the creation of, amongst other applications, an application which uses crowd-sourced data to inject transparency into pricing algorithms. This would also help to address potentially harmful aspects of price discrimination.

Essay (2500 words including footnotes and bibliography)

1. Introduction

Joseph Raz drew an analogy between the law and a knife – both are morally neutral instruments, capable of being put to praiseworthy and nefarious ends.[1] These observations apply to AI. Some problems created by AI are new manifestations of pre-existing ills, whilst other problems require novel solutions. To tackle the hard cases, I suggest that regulatory insights can be gleaned from adjacent fields, and regulators should proactively obtain information about AI tools and engage companies to influence the upstream development of AI. AI tools have significant potential for use in areas such as regulatory enforcement and deployment in applications that promote transparency and consumer choice.

2. Tension?

There is no inherent conflict between protecting competition and consumers and advancing technology. Top AI executives have recognised the importance of developing AI in a pro-social manner. Microsoft's chief executive officer, Satya Nadella, suggested six principles, including maximising efficiencies without destroying dignity and guarding against bias, that should undergird the development of AI.[2] Ashford and Hall have noted that policy interventions assist in fostering breakthrough technological

[1] B1.
[2] B2.

innovations by increasing capacity, opportunity and motivation,[3] and antitrust law assists by opening up the participatory and political space.[4] Regulators thus play an important role in *fostering* AI development along such pro-social lines.

I turn to the *means* through which the government can protect competition and consumers *whilst promoting* technological advancement.

3. The easy cases

AI can facilitate common *existing* types of competition and consumer law violations. Ezrachi and Stucke have written about the use of computers as "messengers" between colluding parties.[5] They have also described a "hub and spoke" scenario where competitors use the same algorithm to determine prices, such that this common algorithm leads to horizontal alignment.[6] The UK Competition & Markets Authority ("CMA") has written about how consumers can be harmed by algorithm-facilitated business practices such as self-preferencing by online platforms to favour their own products at the expense of competitors.[7]

These are easy cases in that such situations can be governed by existing laws. A cartel is still a cartel regardless of whether the agreement to collude is forged between persons meeting or forged using AI exchanging messages. For instance, the CMA acted in 2016 against Trod Ltd for colluding with GB eye Ltd via an automated re-pricing software to monitor and adjust their prices on Amazon, ensuring that neither of the parties was undercutting the other.[8] In another example, Google was fined €2.42

[3] B3 at p 289.

[4] B3 at p 289.

[5] B4 at 1784.

[6] B4 at 1787.

[7] B5.

[8] B6 at paras 24–26.

billion by the European Commission for abuse of its dominant position in general online search by adopting an algorithm that demoted third-party comparison-shopping services in Google search results.[9]

I turn then to the harder issue of *new* problems created by AI.

4. Lessons from adjacent fields

Zheng and Wu have noted that uncertainty involved in complex algorithms makes the outcome of AI collusion unpredictable and uncontrollable, such that regulators face difficulty proving that there is actionable collusion among firms.[10] It has also been observed that there is “tech-legal lag”, where regulators are forever trying to keep pace with AI developments.[11] I suggest that insights on tackling such issues can be gleaned from adjacent fields.

a. Enterprise risk

The notion of “enterprise risk”, long a mainstay of vicarious liability,[12] may provide a good normative foundation for regulatory approaches to AI in the competition and consumer space. “Enterprise risk” refers to the idea that (a) enterprises which engage agents to advance their interests and thereby create risks of agent wrongdoing should bear responsibility when such risks eventuate; and (b) such enterprises are also best placed to, and should be incentivised to, manage their risks and prevent wrongdoing.[13]

There are salient parallels between agents and AI. When companies use AI for their business operations, they are advancing their commercial interests and creating risks.

[9] B7 at [566].
[10] B8 at 146.
[11] B9.
[12] B10 at [153].
[13] B10 at [153].

They should bear responsibility when such risks eventuate, even if the risks were difficult to predict at the outset due to limitations in the current state of technical knowledge. Companies *themselves* are best placed to prevent wrongdoing. Companies which develop their own AI algorithms directly control the programming process, whilst companies that purchase AI tools from others can bargain with the vendor for specifications and make private arrangements (*eg*, indemnity clauses) to account for the risk that AI tools bring. An internet commentator has referred to generative AI tools as an "intern"[14] and this analogy is apt – a company should not escape liability by pinning blame on a rogue intern. There is thus a sound normative basis for holding companies "vicariously" liable if it turns out that their AI tools have caused competition and consumer law infringements.

b. Attribution

Relatedly, it is possible to treat an AI tool as a "rogue agent" whose acts the user is vicariously liable for, even for competition and consumer law prohibitions that require both *actus reus* and *mens rea*. It is well-established in case law that mental states must frequently be inferred from conduct and all other relevant circumstances of the case.[15] I suggest that when an AI tool is personified as a "rogue agent" for the purpose of a doctrine of vicarious liability, regulators and courts can ascribe requisite mental states to the AI tool by examining its conduct and other relevant circumstances. For instance, if some autonomous, internet-enabled AI pricing tools used by different companies were found to routinely upload planned contractual bids into a server accessible by all said tools, and there is evidence that prices in that market are curiously at supra-competitive levels, a regulator may infer that a bid-rigging

[14] B11.

[15] B12 at [97].

conspiracy is afoot as between those AI tools. Even if those AI tools may have *autonomously* learnt such practices through machine learning without being explicitly programmed to do so, a system of vicarious liability could hold the company *using* the AI tool responsible for the tool's misdeeds.

Furthermore, inspiration may be gleaned from the discussion about rules of attribution in *Red Star Marine Consultants*.[16] There are legal rules allowing for the acts and intentions of human agents to be attributed to a company, which has no mind and body of its own.[17] The Court of Appeal in *Red Star Marine Consultants* noted at [37] that there exists special rules of attribution which are "context-specific" with their content "determined based on the language and purpose of the substantive law upon which potential liability is to be established". It is possible, where AI is concerned, for courts and regulators to fashion context-sensitive rules to attribute mental states and actions to AI tools, and in turn for these mental states and actions to further be attributed to the company using the AI tool.

c. Disclosure

The CCCS has extensive powers to require production of information under ss 61A and 63 Competition Act 2004 ("CA"). Such information would include source code and usage logs of AI tools. Section 89 CA further contains rules providing for CCCS to preserve the secrecy of information furnished. By examining AI source code and usage logs – with the assistance of expert opinion if necessary – regulators can form a view as to whether the AI tool can be used or has been used in a manner that infringes competition and consumer law. To the extent that aspects of AI behaviour remain a technological mystery because of limitations in current knowledge, courts

[16] B13.

[17] B13 at [30].

and regulators have routinely dealt with such evidential uncertainty (see, *eg*, *McGhee v National Coal Board* [1973] 1 WLR 1 and the limits of medical knowledge discussed therein). The burden of proof doctrine assists to provide an answer to situations where the limits of current knowledge mean that evidential uncertainty must be resolved against one party or the other.

Relatedly, regulators should encourage candid and proactive disclosures by companies, and be ready to engage in constructive, confidential and even without prejudice dialogue when companies apply for guidance or decisions. Such dialogues offer a chance for regulators to gain access – upstream – to information about the latest developments in commercial AI. The contents of the guidance or decision provided can also shape future development of AI.

Moreover, there is literature demonstrating methods for demystifying machine learning algorithms. Häfner, Gemmrich and Jochum have applied symbolic regression to distil a black-box machine learning model for rogue wave forecasting into a human-interpretable mathematical equation.[18] This suggests that the technical complexity of AI algorithms may not be an insurmountable barrier to understanding their operations and ascertaining if these operations harm competition and consumer policy objectives.

5. AI-assisted enforcement

AI tools allow regulators to churn through large volumes of data quickly and intelligently to mount enforcement actions.[19] In investigations that led to the *Google Shopping* case, the European Commission had to analyse 5.2 terabytes of data.[20] Mills and Whittle have shown that AI tools are proficient at automating aspects of

[18] B14.

[19] B16 at 468–469.

[20] B15.

auditing online environments, such as online marketplaces, for dark patterns (*ie,* unfair design practices that impair consumers' ability to make free choices)[21].[22] Crucially, AI tools may be *superior* to human officers in conducting aspects of auditing work as AI can be programmed to simulate a representative sample of individuals from across the population,[23] ensuring that audits more accurately capture risks posed to consumers from different backgrounds.

6. Pro-consumer transparency

AI can help regulators and consumer associations promote transparency, which promotes consumer choice.

Companies have been using AI to adopt personalised pricing strategies.[24] While personalised pricing strategies may sometimes be normatively acceptable (*eg,* student fares), some personalised pricing strategies may be unjustifiably discriminatory on grounds such as race, religion or gender,[25] and yet other strategies may offend consumers' sense of fairness.[26] For instance, Amazon apologised and issued refunds to angry customers after it was alleged to have offered different prices based on customer data.[27] Cheng and Nowag have argued that AI and big data renders it possible to target price cuts only to marginal customers whilst leaving prices for inframarginal customers untouched.[28] AI therefore brings firms closer to implementing first-degree price discrimination, which would allow firms to capture the entirety of the consumer surplus.

[21] B5; B18 at Art 25(1).
[22] B17.
[23] B17 at p 3.
[24] B19 at paras 29–31.
[25] B5.
[26] B20.
[27] B21.
[28] B22.

I suggest, however, that AI and big data can also allow consumers and regulators to fight back by improving transparency and facilitating informed choice. The Consumers Association of Singapore launched the Price Kaki application in 2019. A key feature of the application is to give the current retail prices of items sold in supermarkets. Price Kaki works based on crowd-sourcing pricing data from consumers, along with data supplied by verified retailers.[29] One can imagine a similar application being launched for digital services.

Take the example of ride-hailing services. An application could crowdsource trip data (such as time, location and price) and send the data to servers where the data is processed using AI. Provided that users consent, the trip data can be matched with a user's personal data found in a user's Singpass Myinfo profile. It would then be possible for a regulator or consumer association to find traces of attempts at first-degree price discrimination. In turn, the broad conclusions drawn from the information could be released to the public for consumers to form their own views on the degree to which they would accept such a pricing model. Consumers would therefore be empowered to speak out, or vote with their wallets.

More broadly, various AI products have been made available to assist consumers. For instance, researchers at Aarhus University have developed "Consent-o-Matic", a browser extension which recognises pop-ups on websites seeking users' consents for data-collection and automatically fills them out based on users' preferences.[30] Regulators and consumer associations can *create* such tools for consumers. In the

[29] B23.

[30] B24.

Singapore context, the uptake of such tools would likely be high as government-related institutions enjoy a high degree of trust[31] and digital literacy is high.[32]

7. Conclusion

AI's morally neutral nature means that it is important for policymakers to develop rules that ensure that AI's deeds or misdeeds can be attributed to a person or entity that can be held responsible. While AI development carries risk, it also carries opportunities which can be exploited by regulators and consumer associations.

Bibliography

B1.	Joseph Raz, *The authority of law: Essays on law and morality*, OUP 1979
B2.	Satya Nadella, "The Partnership of the Future", *Slate*, 28 June 2016
B3.	Ashford, Nicholas & Ralph Hall, "The Importance of Regulation-Induced Innovation for Sustainable Development", Sustainability 3, no. 1 270–292
B4.	Ezrachi A & Stucke M, "Artificial Intelligence & Collusion: When Computers Inhibit Competition" [2017] (5) University of Illinois Law Review 1775
B5.	Competition & Markets Authority, "Algorithms: How they can reduce competition and harm consumers", 19 January 2021
B6.	OECD, "Algorithms and Collusion – Note from the United Kingdom", 30 May 2017
B7.	Case T-612/17 *Google and Alphabet v Commission* EU:T:2021:763

[31] B25.

[32] B26.

B8.	Guan Zheng & Hong Wu, "Collusive Algorithms as Mere Tools, Super-tools or Legal Persons", Journal of Competition Law & Economics (15) 2-3, June/September 2019 123–158
B9.	Wolters Kluwer, "Playing Catch-Up: European Competition Law in the Digital Age", 4 September 2019
B10.	*Ong Han Ling v American International Assurance Co Ltd* [2018] 5 SLR 549
B11.	Economist Writing Every Day, "ChatGPT is your new intern" <https://economistwritingeveryday.com/2023/04/17/chatgpt-as-intern/> 17 April 2023, accessed 26 May 2024
B12.	*Daniel Vijay s/o Katherasan v Public Prosecutor* [2010] 4 SLR 1119
B13.	*Red Star Marine Consultants Pte Ltd v Personal Representatives of Satwant Kaur d/o Sardara Singh, deceased* [2020] 1 SLR 115
B14.	Häfner, Dion *et al*, "Machine-guided discovery of a real-world rogue wave model", Proceedings of the National Academy of Sciences 120 (2023).
B15.	Statement by Commissioner Vestager, 27 June 2017
B16.	Andreas von Bonin & Sharon Malhi, "The Use of Artificial Intelligence in the Future of Competition Law Enforcement", Journal of European Competition Law & Practice, 2020, Vol 11 No 8 468
B17.	Mills, Stuart and Whittle, Richard, "Detecting Dark Patterns Using Generative AI: Some Preliminary Results", *SSRN*, 27 October 2023
B18.	Directive 2000/31/EC (Digital Services Act)
B19.	OECD, "Personalised Pricing in the Digital Era – Background Note by the Secretariat", 20 November 2018

B20.	Brian Wallheimer, “Are You Ready for Personalized Pricing?”, *Chicago Booth Review*, 26 February 2018
B21.	ABC News, “Amazon Error May End 'Dynamic Pricing'”, 29 September 2000
B22.	Thomas Cheng & Julian Nowag, “Algorithmic Predation and Exclusion”, 25 U. Pa. J. Bus. L. 41 (2023).
B23.	Rexanne Yap, “I tested out CASE's Price Kaki app to save money on groceries, it was quite useful”, *Mothership*, 9 March 2020
B24.	Midas Nouwens *et al*, “Consent-O-Matic: Automatically Answering Consent Pop-ups Using Adversarial Interoperability”, CHI Conference on Human Factors in Computing Systems, April 2022
B25.	Chew Hui Min, “Government remains most trusted institution in Singapore, amid global trend of societal polarisation: Survey”, *CNA*, 15 March 2023
B26.	IMDA, “Singapore Digital Society Report 2023”, 16 May 2024