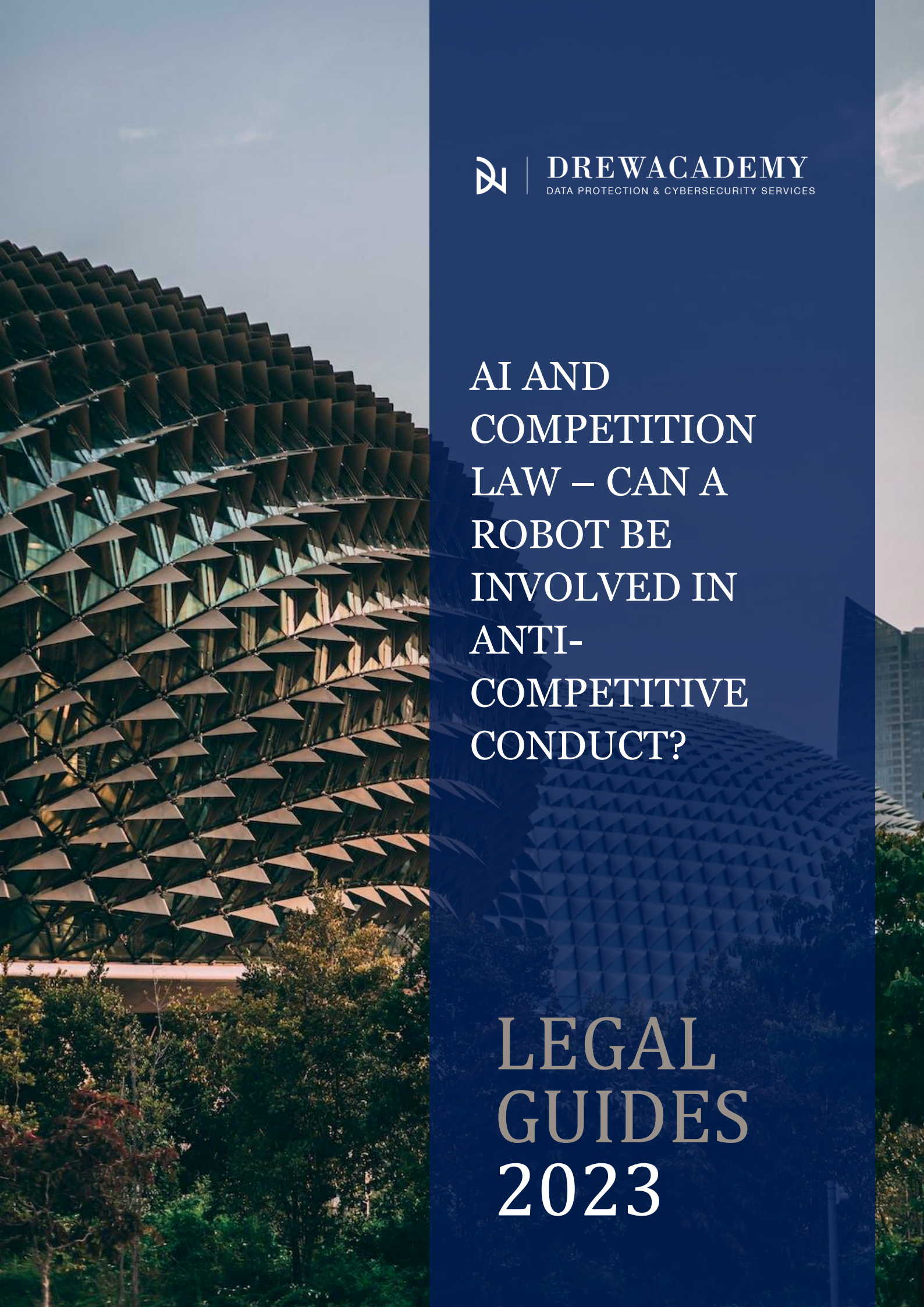

DREWACADEMY
DATA PROTECTION & CYBERSECURITY SERVICES

AI AND COMPETITION LAW – CAN A ROBOT BE INVOLVED IN ANTI-COMPETITIVE CONDUCT?

LEGAL GUIDES
2023

CONTENTS

Developments as of 11 April 2023

DREWACADEMY
DATA PROTECTION & CYBERSECURITY SERVICES

AI AND COMPETITION LAW – CAN A ROBOT BE INVOLVED IN ANTI-COMPETITIVE CONDUCT?

The increased adoption of artificial intelligence ("AI") technologies by corporations in the private sector in recent years has raised several issues in the area of competition law. Corporations should therefore be aware of possible pitfalls and concerns that competition authorities have with respect to the proliferation of AI. This article will discuss four key issues in relation to AI and competition law: algorithmic collusion, personalised pricing, liability for learned collusive behaviour, and the use of AI which reinforces a dominant market power.

Algorithmic collusion

The use of AI tools has expanded not only the manner and possibility of collusion but the grey area between unlawful explicit collusion and lawful tacit collusion as corporations may not need to communicate with each other to collude. The most common example of AI tools being used in the market is pricing algorithms. Pricing algorithms include algorithms that monitor and extrapolate trends in prices in the market and those that are able to weigh information like supply and demand and competitor's pricing to make real-time adjustments to prices.

As highlighted by the Organisation for Economic Co-operation and Development ("OECD"), a corporation's individual use of a pricing algorithm is not illegal as it would "fall squarely into the box of intelligent adaptation to observed market behaviours of competitors and normal market interdependence".[1] However, the question that arises with respect to the use of such sophisticated pricing algorithms that are able to anlayse competitors' prices and make adjustments is whether, when used by multiple corporations in the market, the use can constitute unlawful collusion. While each corporations' decision to implement pricing software is, in and of itself not unlawful, there are two situations in which they may fall afoul of competition law.

The first situation is where firms have an explicit agreement to collude and use pricing software to implement their agreement. The 2015 US case of *U.S.A. v David Topkins*[2] is illustrative in this situation. Topkins, a director of a company that sold posters online, was held liable for price fixing with other merchants on Amazon Marketplace. Topkins had agreed with other merchants on the levels of prices and the specific algorithm to be used by the merchants to coordinate prices on their posters. The use of pricing algorithms was not illegal but the existence of the agreement to jointly implement the algorithm made the case for the Department of Justice. Therefore, it is clear that unlawful collusion will be found where pricing algorithms are used in concert and to facilitate explicit agreements. Singapore's competition authority, the Competition and Consumer Commission of Singapore ("CCCS"), has also cautioned corporations against this and stated that AI or algorithms used to support or facilitate any pre-existing or intended anti-competitive agreement will be subject to the prohibition against agreements that prevent, restrict or distort competition under section 34 of the Competition Act 2004.[3]

The second situation is where corporations use the same pricing algorithm from the same service or product provider. This may create an unlawful hub-and-spoke scenario where coordination, knowingly or not, between corporations in the same market is caused by using the same "hub" for obtaining pricing algorithms to implement their pricing strategies.

Where corporations innocently use such pricing algorithms, competition authorities have yet to conclusively decide if this falls afoul of competition law. Notably, the UK's Competition and Markets Authority ("CMA") has found that the risks of collusion in such a scenario are unclear due to relatively little empirical evidence and there is thus no answer yet as to whether competition authorities can object to such hub-and-spoke and autonomous tacit collusion situations where there is neither direct contact between competitors nor a meeting of minds between them to restrict competition.[4] Some academics have suggested that in such scenarios, the competition authority may have to delve into the heart of the

[1] See "*Roundtable on Hub-and-Spoke Arrangements – Background Note"* by OECD (2019) at paragraph 105.
[2] https://www.justice.gov/atr/case-document/file/513586/download
[3] See "E-commerce Platforms Market Study", CCCS (2020) at paragraph 217.
[4] See "*Algorithms: How they can reduce competition and harm consumers*" by UK CMA (2021) at paragraph 2.87.

algorithm and establish if it is designed in a way to facilitate collusion among its users.[5] If this is established, it would be an unlawful hub-and-spoke scenario.

In Singapore, while this issue has not been raised, the CCCS has considered that where each corporation uses a distinct algorithm with no prior or ongoing communication, but achieves an alignment of market behaviour, there is no clear consensus on how collusive outcomes may be achieved. As such, the assessment of whether collusive outcomes can be attributed to the corporations will be decided on a case-by-case basis.[6] One possible consideration could be whether the corporations were aware of the anti-competitive conduct but chose not to distance themselves from it such as in the case of *Eturas UAB and Others v Lietuvos Respublikos konkurencijos taryba* which was decided by the European Court of Justice ("ECJ")[7].

Personalised pricing

With the use of AI, corporations can process the data they have on consumers and their characteristics. AI that is able to generate inferred data such as brand loyalty, consumption preferences and purchasing behaviour will potentially allow corporations to set individually tailored prices based on a consumer's willingness to pay using the collected data points.[8] The question that arises is whether this practice could constitute an exploitative abuse when used by a corporation that has a dominant position in the market and thus, infringe section 47 of the Competition Act 2004[9].

An exclusionary abuse of dominance may arise where corporations use AI to identify consumers of rival products and implement personalised pricing to lure consumers away from competitors. However, the OECD has noted that, at present, the risk and extent of personalised pricing in real markets remains largely unknown due to a lack of reported cases since corporations are not transparent about their pricing strategies.[10] Furthermore, personalised pricing may not necessarily be a cause for concern to competition authorities. Personalised pricing can potentially benefit consumers by improving accessibility of products and creating market efficiency. For instance, the use of AI to determine consumer willingness to pay could lead to lower prices being offered to some consumers which are offset by higher prices for consumers who have a greater willingness to pay.[11]

Nonetheless, the CCCS has stated that personalised pricing may infringe section 47 of the Competition Act 2004 where there is evidence that it is used to harm competition. Specifically, the CCCS highlighted that section 47 will be infringed where a dominant corporation uses personalised pricing to set discounts that have the effect (or likely effect) of foreclosing all, or a substantial part, of a market.[12]

Liability where AI learns collusive behaviour

Presently, most AI systems operate based on instructions from humans and are treated as a "tool" to improve efficiency and delivery of services. Therefore, decisions made by an AI system can be directly attributed to its human operators. However, as AI develops, the link between the AI and the human operator will likely become weaker as machine learning advances. If AI advances to a stage where it autonomously learns and implements anti-competitive and collusive behaviour, the issue is how

[5] See by Ezrachi and Stucke (2017) at page 1788.
[6] See "E-commerce Platforms Market Study" by CCCS (2020) at paragraph 214.
[7] This case concerned travel agencies coordinating discount rates through the system administrator of a common computerized booking system. The ECJ stated that if competitors were aware of the system administrator's message to impose a cap on discount rates and they did not publicly distance themselves from the practice, this would be a concerted practice contrary to competition law.
[8] See "*OECD Business and Finance Outlook 2021: AI in Business and Finance*" by OECD (2021).
[9] Section 47 of the Competition Act 2004 prohibits corporations from abusing their dominant position in the market and includes conduct such as predatory behaviour towards competitors and limiting product, markets or technical development to the prejudice of consumers.
[10] See "*Personalised Pricing in the Digital Era – Background Note*" by OECD (2018) at paragraph 6.
[11] *Supra* note 8.
[12] See "E-commerce Platforms Market Study" by CCCS (2020) at paragraph 162.

competition authorities should attribute liability considering that there may be no communication between competitors and AI systems.

While this is still a largely theoretical debate, the UK's CMA has stated that firms are responsible for the effective oversight of AI systems which include robust governance, holistic impact assessments, monitoring and evaluation.[13] Similarly, in Singapore, guidance can be taken from the Infocomm Media Development Authority ("IMDA") and Personal Data Protection Commission's ("PDPC") second edition of the Model Artificial Intelligence Governance Framework. The Model AI Governance Framework suggests that corporations should adhere to principles such as responsibility, accountability and transparency when using AI, which includes being able to explain decisions made by AI. As such, corporations in Singapore may not be able to disclaim responsibility for the decisions made by such autonomous AI. The Australian Competition and Consumer Commission has pithily summed up the debate by stating that "we take the view that you cannot avoid liability by saying "my robot did it"."[14]

AI reinforcing a dominant market power

In the case of corporations in a dominant market position, AI can be used to abuse their dominant market power. This is especially so where a dominant, vertically integrated platform could use AI to systematically favour its own downstream products or services and limit the opportunity for competitors to compete. A related example of this is the European Commission's decision against Google.[15] The European Commission found that Google provided an "illegal advantage" to its own comparison shopping service by pushing the products of rivals further down in its search results and presenting its own service in a more favourable position. Therefore, Google was found to have leveraged its position in the market and its self-preferencing conduct foreclosed competing comparison shopping sites from the market which reduced consumer choice.

Another issue that arises stems from the data-driven nature of AI. AI is trained on data, and the more data it has to draw inferences from, the more likely it is to provide more relevant and personalised outputs for consumers. Where firms are already a dominant market power, they will have exclusive access to a large volume of consumer data and increased AI capabilities to create highly tailored services. Dominant market powers will thus be reinforced and raise the barriers to entry if it limits realistic opportunities or reduces incentives for consumers to switch to competitors who may not be able to provide similarly personalised services.[16]

The refusal to share data sets by a dominant market power may also be an abuse of dominance under section 47 of the Competition Act 2004. The CCCS has acknowledged that the control or ownership of data is a key factor in determining market power[17] and a refusal to supply data by a dominant corporation may be considered an abuse if there is evidence of (likely) substantial harm to competition and if the behaviour cannot be objectively justified[18].

In conclusion, corporations should first and foremost be alive as to how any AI they choose to deploy functions and keep up with guidelines released by local regulators such as the CCCS and IMDA/PDPC. Corporations that are dominant market powers should also take extra care to ensure that they do not use AI in a manner that abuses their dominance in the market.

Drew Academy wishes to acknowledge our Associate Julian Liaw for assisting in the preparation of this article.

[13] See "*Algorithms: How they can reduce competition and harm consumers*" UK CMA (2021) at paragraph 1.6.
[14] See "The CCC's approach to colluding robots address" by ACCC (2017), available at: https://www.accc.gov.au/about-us/media/speeches/the-accc%E2%80%99s-approach-to-colluding-robots-address.
[15] Case AT.39740 Google Search (Shopping).
[16] See "*Algorithms and Collusion – Note from the UK*" by OECD (2017) at paragraph 32.
[17] See "Guidelines on the Section 47 Prohibition" by CCCS (2022) at paragraph 9.4.
[18] See "Guidelines on the Section 47 Prohibition" by CCCS (2022) at paragraph 11.34.

DREW DATA PROTECTION & CYBERSECURITY ACADEMY

Drew Data Protection & Cybersecurity Academy (Drew Academy) was established in 2020 by Drew & Napier to help our clients build their capabilities and develop and implement organisational strategies, structures, policies and processes to meet their legal, regulatory and compliance obligations. Drew Academy offers a range of courses in areas such as data protection, cybersecurity, data governance and in-house commercial practice. A particular focus for us is the delivery of workplace learning solutions and development of customised training courses. We also offer outsourced DPO services and data protection consulting services through our experienced team of practitioners.

Drew Academy is helmed by Lim Chong Kin and David N. Alfred. Our course leaders are experienced in various aspects of data and cyber governance, data protection, cybersecurity engineering and in-house commercial practice.

ARTIFICIAL INTELLIGENCE AND DIGITAL TRUST

Drew & Napier's Artificial Intelligence (AI) and Digital Trust practice brings together its expertise across several technology-related domains and in fields as diverse as data protection, cybersecurity, healthcare, Fintech, intellectual property and competition law (to name a few) to advise clients on the full range of legal issues relating to AI and Digital Trust. In addition to advising on commercial, regulatory and international / cross-border issues, our advice extends into areas such as governance and ethics as we seek to enable our clients to navigate areas where laws and legal principles are still emerging.

Working together with the Drew Academy, we provide solutions that reflect our deep understanding of underlying technologies, the risks and uncertainties involved and practical business considerations. Internationally, there is a growing consensus on AI governance.

For more information on our experience, please contact:

Lim Chong Kin
Managing Director, Corporate & Finance;
Co-Head, Data Protection,
Privacy & Cybersecurity Practice;
Co-Head, Drew Data Protection &
Cybersecurity Academy

T: +65 6531 4110
E: chongkin.lim@drewnapier.com

Corinne Chew, Dr
Director, Corporate & Finance;
Co-Head, Competition Law & Regulatory Practice

T: +65 6531 2326
E: corinne.chew@drewnapier.com

David N. Alfred
Director, Corporate & Finance;
Co-Head, Data Protection,
Privacy & Cybersecurity Practice;
Co-Head and Programme Director,
Drew Data Protection &
Cybersecurity Academy

T: +65 6531 2342
E: david.alfred@drewnapier.com

Cheryl Seah
Director, Corporate & Finance

T: +65 6531 4167
E: cheryl.seah@drewnapier.com

DREWACADEMY
DATA PROTECTION & CYBERSECURITY SERVICES

10 Collyer Quay
10th Floor Ocean Financial Centre
Singapore 049315

www.drewnapier.com/Academy

T: +65 6531 4152
F: +65 6535 4864
E: academy@drewnapier.com

In association with

DREW & NAPIER