Artificial intelligence, algorithms and antitrust
Suzanne Rab*

Abstract: The field of artificial intelligence or ‘AI’ has been reshaping virtually every industry built on the idea that machines could be used to simulate human intelligence through so-called ‘machine learning’. Antitrust interest in this topic has been generated among regulators, policy-makers, academics and business in the EU and internationally. This article explores the extent to which AI may raise competition or other concerns for consumer welfare and whether existing legal and policy instruments are appropriate to deal with the emerging opportunities and challenges.

Keywords: artificial intelligence, AI, algorithms, antitrust, Big data, tacit collusion, digital

1. Introduction
The debate around artificial intelligence or ‘AI’ has attracted antitrust interest among policy-makers, regulators, practitioners and academics and, as yet, there is no consensus internationally on the extent to which existing law and policy is fit for purpose. In their book, Virtual Competition, Professors Ariel Ezrachi and Maurice Stucke postulate the ‘end of competition as we know it’ and call for heightened regulatory intervention against algorithmic systems.1

The AI antitrust literature reflects three broad themes or postulated areas of antitrust concern. First, it is suggested that AI can broaden the circumstances in which known forms of anti-competitive conduct, and particularly conscious parallelism or tacit collusion,2 can occur. Secondly, it is hypothesized that the use of algorithms will bring newer forms of anti-competitive conduct which challenge traditional antitrust orthodoxy with new elements such as price discrimination, co-opetition,3 data extraction and data capture. Thirdly, it is suggested that deception is inherent in algorithmic markets, prompting consumers to engage in exploitative transactions.

As the technology itself is continuing to develop, this article focuses on the claimed facilitating role of algorithms, whether they may contribute or lead to anti-competitive outcomes and the implications for policy and antitrust intervention. It considers: (1) whether AI leads to anti-competitive outcomes or other consumer welfare concerns, (2) whether there is an enforcement gap, and (3) views from the regulators on attribution of liability for AI decisions.

2. Mapping out the subject matter

2.1. Evolution and characteristics of AI
The field of AI as a discrete phenomenon has its origins in a workshop organized by John McCarthy held at Dartmouth College in 1956.4 The aim of the workshop was to explore how machines could be used to simulate human intelligence. Various disciplines contribute to AI including computer science, economics, linguistics, mathematics, statistics, evolutionary biology, neuroscience and psychology. A number of factors, including trends in the use of ‘Big data’ have contributed to innovations in AI but have raised new challenges about automation and its impact on society and the economy.

2.2. Taxonomy
There is no single or universally accepted definition of AI, but there are different definitions and taxonomies. To assist in mapping out the subject-matter, it is useful to consider how AI relates to other key conceptual and analytical frameworks.

---

* Barrister, Serle Court Chambers, London and Professor of Commercial Law and Practice Chair, Brunel University London.


2 Tacit collusion is a form of collusion typically seen in an oligopolistic market structure, where competing firms providing a good do not explicitly collude on any feature (such as price, quantity, or product characteristics), but rather, observe and imitate each other’s actions in a way that is mutually beneficial to both sides.

3 Co-opetition involves collaboration between competitors, in the hope of mutually beneficial results.

a. Artificial intelligence
A useful starting point is a definition offered by Russel and Norvig where, for example, AI is defined as computers or machines that seek to act rationally, think rationally, act like a human, or think like a human.\textsuperscript{5}

AI is therefore characterized by four main features:

- Acting rationally: AI is designed to achieve goals via perception and taking action as a result.
- Thinking rationally: AI is designed to logically solve problems, make inferences and optimize outcomes.
- Acting like a human: This form of intelligence was later popularized as the ‘Turing Test’, which involves a test of natural language processing, knowledge representation, automated reasoning and learning.
- Thinking like a human: Inspired by cognitive science, Nilsson defined AI as that activity devoted to making machines intelligent, and intelligence is that quality that enables an entity to function appropriately and with foresight in its environment.\textsuperscript{6}

A further distinction may be made between ‘narrow’ and ‘general’ AI. Narrow AI concerns applications that provide domain-specific expertise, or task completion. General AI refers to an application that exhibits intelligence comparable to a human, or that outperforms humans, across the range of contexts where humans interact.

b. Machine learning
The early implementations of AI mainly comprised systems within a narrow area and were programmed by human experts. The central focus of more recent developments in AI is around machine learning (‘ML’) systems. In contrast to expert systems, ML algorithms and systems are trained against observational or simulated outcomes.

ML applications of AI include natural-language processing and computer vision. Examples of natural language processing include machine translation, personal assistants and smart phones. Examples of computer vision include algorithms and technologies used to understand scenes, which may be captured by any one or a combination of cameras, radar lasers etc.

c. Big data
The debate around AI has often been linked with discussions around data and, more specifically, ‘Big data’. The term ‘Big data’ has been coined for the aggregation, analysis and increasing value of vast exploitable datasets of unstructured and structured digital information. Big data is characterized by three main characteristics:

- Aggregation in terms of size, shape (e.g. text, image, video, sound), structure and speed.
- Analysis: Big data concerns aggregated datasets which are analysed by quantitative analysis software (using AI, ML, neural networks, robotics and algorithmic computation) on a real-time basis.
- Increasing value: It will facilitate small but constant, fast and incremental business change and enhance competitiveness, efficiency and innovation and the value of the data used.

d. Personal data
As a sub-set of data, it is useful to distinguish personal data. This term has a legal significance under data protection law and, specifically, under the EU General Data Protection Regulation (‘GDPR’).\textsuperscript{7} The GDPR does not apply to data that does not relate to or identify an individual, such as aggregated datasets on general trends without identifying people or commercial data such as revenue figures which do not contain personally identifiable information. Certain categories of personal data are treated as more sensitive and require greater protection under the GDPR.\textsuperscript{8}

Data can also be ‘pseudonymised’. Pseudonymised data is personal data that has been processed so that it can no longer be attributed to a specific data subject without the use of additional information such as a unique identifier which can make the data identifiable. An original data set even without the identifier can still be personal data (in the hands of an organization that holds both the data set and the identifier) since it can be matched with the original database to make the data identifiable. In order to become pseudonymised data, the additional information must be kept separately

---


\textsuperscript{7} Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) O.J. 2016 L 119/1 (GDPR).

\textsuperscript{8} The personal data requiring greater protection under the GDPR may be grouped into the following broad categories: Special categories of data. Special categories of data are, for the purposes of processing under the GDPR: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purposes of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation (Article 9(1), GDPR). Criminal conviction and offence data. Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority (Article 10, GDPR).
and held subject to adequate technical and organizational measures. The data can then be considered as pseudonymised data even where the identifier is kept within the same organization. Pseudonymised data remains personal data but pseudonymisation provides a security mechanism for reducing the level of risk exposure under the GDPR.

3. Does AI lead to anti-competitive outcomes?

3.1. Hypothesis (1): will AI facilitate collusion?

The main concern raised to date in the context of competition law is that a specific type of AI – specifically pricing algorithms used by firms to monitor, recommend, or set prices – can lead to collusive outcomes in the market in two particular ways. First, it is suggested that these pricing algorithms may help facilitate explicit coordination agreements among firms. This is based on the premise that the use of algorithms may make market conditions more suitable for coordination. For example, monitoring prices of other firms could be easier when algorithms are deployed and AI could also be used to implement coordination agreed between humans. Secondly, it is suggested that, under certain conditions, the use of pricing algorithms can facilitate tacit collusion even absent an agreement. This is based on the premise that when many or all firms in the market use similar algorithms to set prices, their strategies can be anticipated by each other, making it easier to reach coordinated outcomes.

Mehra has focused on the facilitating role of algorithms in tending towards conscious parallelism, stating that:

... to the extent that the effects of oligopoly fall through cracks of antitrust law, the advent of the robo-seller may widen those cracks into chasms. For several reasons, the robo-seller should increase the power of oligopolists to charge supra-competitive prices: the increased accuracy in detecting changes in price, greater speed in pricing response, and reduced irrationality in discount rates all should make the robo-seller a more skilful oligopolist than its human counterpart in competitive intelligence and sales ... the robo-seller should also enhance the ability of oligopolists to create durable cartels.

This suggests that algorithms can be a ‘plus factor’ which renders tacit collusion more likely, stable and durable by facilitating detection and retaliation at lower levels of concentration than traditional theory would hold. However, this claim is not straightforward and invites further examination. Firms would still need to choose whether to use and continue to use the same or similar algorithms. The incentive to coordinate is not automatic just because algorithms exist. Firms could still choose to undercut rivals even where they deploy algorithms as part of price-setting. Indeed, smart algorithms might even try to cheat without being caught. Some of the alternative hypotheses are shown in Table 1 below, which considers some of the typical market conditions preventing coordination and aspects of AI which may count as factors making coordination more or less likely.

It follows that the hypothesis that algorithms may make tacit collusion more likely requires further examination. First, where transactions are more personalized – as they increasingly tend to be in the digital economy – each transaction with the customer may be seen as a ‘one shot game’ which is inconsistent with tacit collusion. Secondly, where non-price competition is included with elements such as differential service and quality standards, there is more background ‘noise’. This, in turn, may tend to make detecting and punishing deviations more costly. Finally, there is currently limited understanding of countervailing strategies. Buyers – or even AI systems on the buy-side – may be able to counteract oligopolistic pricing that disrupts the sellers’ algorithms. The fast-moving pace of technology may suggest a prospect of the emergence of AI countervailing measures which invite or facilitate new entry, for example, through data perturbation,10 masking,11 encryption and other variants.

3.2. Hypothesis (2): Will AI lead to other outcomes which present concerns for consumer welfare?

A further theme in the antitrust debate is that algorithmic markets will tend to increase price transparency and mean that customers are nudged into deceptive or exploitative personalized pricing. These propositions and whether they are likely to be harmful need to be tested.

It may be conjectured whether access to Big data will genuinely increase price transparency and whether the outcomes are necessarily anti-competitive. There is at least an alternative hypothesis to be tested that firms may compete on building customer relationships where the outcomes are more rather than less

10 Data perturbation is a data security technique that modifies the database to preserve the privacy and confidentiality of the data.
11 Data masking is a method of creating a structurally similar but inauthentic version of an organization’s data that can be used for purposes such as user training or software testing.
Further, price discounts may be offered via encrypted communications direct to customers. AI systems are in any event capable of encryption. The result may therefore be equivocal for price transparency and consistent with competitive pricing.

As to the relationship between AI and personalized pricing, in the digital economy products are becoming increasingly differentiated with competition around non-price elements, including service, quality and even data privacy. The result may be heterogeneous products, offered as a service. In these circumstances it may be harder for algorithms to compare genuine ‘like for like’ prices. The result may actually be more innovation, more and increasingly sophisticated differentiated products, products-as-a-service, and customer-specific pricing that is largely pro-competitive.

### 3.3. Hypothesis (3): Will AI lead to other (not necessarily anti-competitive) outcomes?

AI in general generates a wide range of efficiencies. For example, AI can be used to predict demand using historic data and help businesses to improve their inventory management. AI may be effective in replacing human labour for simple and repetitive tasks in some sectors of the economy. As a result, AI may have impacts on the demand for labour. For example, to develop the performance of and to deploy algorithms, more computer analysts may be required, while the number of manufacturing jobs may reduce as more straightforward tasks can be performed by machines. This is but one example of the potential increase in demand for goods and services that are complementary to the use of AI and AI systems (e.g. computing) and a reduction in demand for goods and services that can be substituted by AI (e.g. bricks and mortar travel agents).

### 4. Is there a policy or enforcement gap?

Accepting the proposition that AI may facilitate at least some outcomes which have attracted antitrust scrutiny, it may be asked whether there might be an enforcement gap in relation to parallel pricing or personalized pricing by or using AI systems.

#### 4.1. Parallel pricing

Ezrachi has questioned whether parallel pricing, to the extent that it may be facilitated by AI, would be caught by EU competition law on restrictive agreements (under Article 101(1) TFEU) at all. This invites consideration of the extent to which the current scope of Article 101 is

<table>
<thead>
<tr>
<th>Market conditions preventing coordination</th>
<th>Aspects of AI facilitating coordination</th>
<th>Alternative hypothesis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Large number of sellers (the greater the number of sellers, the greater the probability that individual sellers will ignore their rivals)</td>
<td>AI may facilitate co-ordination even among a larger number of sellers. Where many or all firms in the market use similar algorithms to set prices, their strategies can be anticipated by each other, making it easier to reach coordinated outcomes</td>
<td>Firms could still choose to undercut rivals for short-term gain; smart algorithms may try to cheat</td>
</tr>
<tr>
<td>Time lag between initial price cut and response of rivals (enables concealment of price reductions, leading to delays in retaliation)</td>
<td>AI may be used to detect and respond to deviations where there is access to Big data</td>
<td></td>
</tr>
<tr>
<td>High discount rate of future profits (provides incentives to appropriate profits in the near-term)</td>
<td>AI may prefer long-term profit maximization</td>
<td></td>
</tr>
<tr>
<td>Misinterpretation of shocks to demand or supply as deviations (leads to inappropriate signalling)</td>
<td>AI may be able to recognize the genuine cause of price reductions</td>
<td></td>
</tr>
<tr>
<td>Different cost structures (where overhead costs are high, pricing discipline tends to break down)</td>
<td>Cost data may become more accessible</td>
<td>AI in principle has no impact on cost structures including the incentive to discount</td>
</tr>
<tr>
<td>Product heterogeneity (the greater the heterogeneity, the more difficult it is to coordinate)</td>
<td></td>
<td>AI does not of itself affect product heterogeneity; individualized pricing could undermine coordination</td>
</tr>
</tbody>
</table>

Source: Author’s own analysis.
adequate to deal with the potential competition issues presented by AI.

Where AI is used by sellers and buyers to anticipate price trends, or using encryption, this resembles a public marketplace. This activity (in the absence of explicit collusion, price signalling or outsourcing of pricing to common agents or intermediaries) is not generally a competition law concern. By analogy, obtaining competitor price data via customers is normally permitted (subject to the comments below on ‘hub-and-spoke’ arrangements).

Cases involving information exchange raise special and often difficult considerations. The European Commission has summarized the evolving case law and its approach to the competition issues arising in information exchange between competitors in its Horizontal Cooperation Guidelines.\textsuperscript{12} A distinction should be drawn between: (a) the exchange of information to monitor a cartel, which is always unlawful; and (b) ‘pure’ information exchange which may, depending on the facts, be lawful.

Existing antitrust tools seek to address some potential anti-competitive effects of information exchange which may be relevant to AI platforms if they act as a hub for systematic information exchange (so-called ‘hub and spoke’ pricing). According to this principle, when information on price is exchanged between two or more undertakings operating at the same level of the supply or distribution chain (A and C) via a common trading contractual party (B) operating at a different level in the supply chain, there can be said to exist horizontal price fixing agreements between the retailers (A and C) themselves.

The Court of Appeal has been satisfied that A, B and C can be seen as parties to a single infringement, as opposed to independent vertical agreements:

\textit{... if (i) retailer A discloses to supplier B its future pricing intentions in circumstances where A may be taken to intend that B will make use of that information to influence market conditions by passing that information to other retailers (of whom C is or may be one), (ii) B does, in fact, pass that information to C in circumstances where C may be taken to know the circumstances in which the information was disclosed by A to B and (iii) C does, in fact, use the information in determining its own future pricing intentions. (emphasis added)\textsuperscript{13}}

### 4.2. Personalized pricing

The European Data Protection Supervisor (‘EDPS’)\textsuperscript{14} notes in EDPS Opinion No 8/2016, in relation to personalized pricing that:

Recent studies have pointed to the potential in the future of machine-learning algorithms to achieve perfect first degree price discrimination, with firms segmenting the market into each individual consumer and charging him according to his willingness to pay. In the near future, technology could potentially enable tacit collusion between companies in digital markets to fix prices through data and self-learning algorithms.\textsuperscript{15}

It is important to distinguish, first, personalized pricing for the same product and secondly, differential pricing for customized products and services. Where pricing reflects the costs and specific features of customized products and services, including the efficiencies arising in selling to that customer, it is difficult to see how this should be an antitrust concern at all. A more interesting inquiry may be made where there is personalized pricing for the same product or service and whether this may lead to customers being nudged into exploitative transactions.

Discriminatory treatment of its customers by a dominant company may infringe Article 102 TFEU as a specific category of abuse. Price discrimination consists of charging different prices to customers in the same position without justification, or charging uniform prices to customers whose circumstances are different.

A challenge may be made to a dominant company’s pricing where the absence of cost differences in supplying individual customers is readily apparent. Key elements of discriminatory pricing include the principles that:

1. prices need not be identical;
2. any differences must be justified by objective and not discriminatory reasons;
3. any charge must not be arbitrary;
4. in the event of disparity, it is for the allegedly dominant company to justify its reasons for the differences; and
5. it is irrelevant that the effects take place in another market provided that the discrimination takes place in a market where the company is dominant.\textsuperscript{16}

---

\textsuperscript{12} Communication from the European Commission – Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal co-operation agreements, O.J. 2011 C11/1 (‘Horizontal Cooperation Guidelines’).

\textsuperscript{13} JJB Sports plc v Office of Fair Trading, Allsports Limited v Office of Fair Trading [2006] EWCA Civ 1318, para 141.

\textsuperscript{14} The European Data Protection Supervisor (‘EDPS’) is the EU’s independent data protection authority.


\textsuperscript{16} See, further, Case C-82/01 Aeroports de Paris v Commission EU:C:2002:61 and section C (priced-based exclusionary conduct), Communication from the European Commission: Guidance on its enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings, O.J. 2009 C45/7 (Article 82 ‘Priority Guidance’).
Although differentiated pricing structures of a dominant firm have raised competition concerns in the past\textsuperscript{17} it may be more challenging to establish discriminatory pricing cases in the future given increasing recognition of the potential objective justification for these structures. However, to the extent that there is an enforcement issue at all, this probably relates to deficiencies in the antitrust framework for dealing with price discrimination and not any special feature of AI.

On the issue of price discrimination by a non-dominant firm, as a threshold observation, dynamic or personalized pricing may enhance overall efficiency even if some individual consumers are harmed. Price discrimination can improve efficiency. In circumstances where pricing approaches marginal revenue, average total costs tend to fall as production expands. This, in turn, may be expected to yield savings arising from economies of scale. The results may be equivocal but are generally increased output and cost savings.

However, dynamic pricing may also give rise to welfare concerns. As a general observation, it is noted first, that the effects of price discrimination are highly dependent on the competitive environment in which it is implemented. Secondly, the harmful effects from personalized or customized pricing are more likely when: (a) it is carried out by a monopolist, (b) the form of price discrimination is complex and/or consumers are unaware of it, (c) it is costly to implement and so it increases costs (but, this is probably less likely to be the case with AI), and (d) it leads to a reduction in consumers’ trust in online markets.\textsuperscript{18}

Recent cases of differential pricing have attracted criticism despite claims of some efficiency benefits. This includes, for example, inquiries into Uber’s ‘surge’ pricing.\textsuperscript{19}

However, this is an area in which to tread carefully and where regulators are largely in evidence gathering and analysis mode. As a note of caution, antitrust interventions which limit product diversity may actually be counterproductive. For example, the CMA’s Final Report on its Energy Market Investigation\textsuperscript{20} found that earlier regulatory intervention to simplify pricing (i.e. Ofgem’s Retail Market Reform rules in 2010) had had an adverse effect on price competition (as well as product differentiation). The CMA stated that: ‘RMR rules, more generally, dampen price competition by limiting the ability and incentives of suppliers to respond to competition by offering cheaper tariffs or discounts (which means that they, in turn, put less competitive pressure on their rivals)’.\textsuperscript{21}

Against the above brief analysis, it appears that we still lack a full understanding of the nature of harm arising from dynamic or personalized pricing – more generally and where AI is involved. Further, it is important to distinguish the nature of the harm arising and whether this is a harm to competition or whether concerns relate more to consumer protection.

Consumer protection, loosely described, aims to address market wide problems or issues which affect consumers’ ability to make effective choices. Competition law and consumer policy are often linked. As the CMA stated in its Consumer Protection Enforcement Guidance:

> Theory and experience strongly suggest that competition and consumer issues are closely linked. Good consumer outcomes rely on competitive markets to provide choice and value, while vibrant competition relies on consumers shopping around.\textsuperscript{22}

The interplay between consumer protection and competition law is important, not least because there will often be a policy determination as to which tools are more appropriate in a given case. Further, there can be a tension or confusion between the application of competition law in relation to unilateral commercial practices such as certain pricing practices (which may be challenged as an abuse of a dominant position when practised by a dominant company) and the obligations of individual businesses under consumer protection law.

There are a number of legal and policy tools that may be deployed to address the threshold concerns arising with personalized pricing including but not limited to antitrust, some of which are identified in Table 2 below.

5. Approach from the regulators

AI and algorithms have attracted interest from antitrust regulators internationally. As yet views tend to be divided on the implications for liability and appropriate enforcement tools. This brief (and necessarily high level

\textsuperscript{17} See, e.g., Aeroports de Paris (In 16).


\textsuperscript{19} During periods of excessive demand or scarce supply, when there are far more riders than drivers, Uber increases its normal fares with a multiplier whose value depends on the scarcity of available drivers. See, further: ‘Surge pricing: How it works and how to avoid it’ (BBC, 15 January 2018), available at: https://www.bbc.co.uk/news/av/business-42661404/surge-pricing-how-it-works-and-how-to-avoid-it.


\textsuperscript{21} Energy Market Investigation (In 20), para 175.

\textsuperscript{22} CMA, Consumer Protection: Enforcement Guidance (17 August 2016) (CM58) (‘Consumer Protection Enforcement Guidance’), para 2.2.
and incomplete) survey nevertheless indicates some anxieties about the ability of traditional enforcement tools to tackle the range of possible outcomes in the absence of evidence of explicit collusion.

### Table 2 Regulatory measures addressed at personalized pricing

<table>
<thead>
<tr>
<th>Measure</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>(1) Competition law</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Abuse of dominance</strong></td>
<td>Article 102 TFEU: Price discrimination by a dominant firm. However, price discrimination cases are rare and tend to arise in relation to discrimination against other trading partners and not individual consumer pricing.</td>
</tr>
<tr>
<td><strong>Market studies and sector inquiries</strong></td>
<td>Using the procedure to identify adverse effects before regulating, e.g.: European Commission E-Commerce Sector Inquiry,(^{23}) and the CMA Market Study on Digital Comparison Tools.(^{24})</td>
</tr>
<tr>
<td><strong>Improving price transparency</strong></td>
<td>Adopting measures to promote price comparison sites and countervailing measures on the buy-side, e.g.: the CMA Final Report on Private Motor Insurance: remedies included giving consumers more transparent information about no claims bonuses.(^{25})</td>
</tr>
<tr>
<td><strong>(2) Other areas (e.g. vulnerable consumers)</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Consumer protection law</strong></td>
<td>Directive 2005/29/EC concerning unfair business-to-consumer commercial practices.(^{26}) This protects consumers against all forms of unfair commercial practices.</td>
</tr>
<tr>
<td><strong>Equality legislation</strong></td>
<td>Existing law protects against certain types of discrimination. The Equality Act 2010 makes it unlawful for a firm to discriminate against a person using or seeking to use its services because of a protected characteristic (age; disability; gender reassignment; marriage and civil partnership; pregnancy and maternity; race; religion or belief; sex; sexual orientation).</td>
</tr>
<tr>
<td><strong>Data protection</strong></td>
<td>Article 22, GDPR: ‘The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.’ Suitable safeguards should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision. As a result, sellers must inform data subjects about personalizing prices.</td>
</tr>
<tr>
<td><strong>(3) General</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Ethics</strong></td>
<td>2017 Asilomar principles.(^{27}) European Parliament Resolution of 16 February 2017 on Civil Law Rules on Robotics (including an Annex on ethical design).(^{28})</td>
</tr>
<tr>
<td><strong>Self-correcting market-led measures</strong></td>
<td>Consumer actions in response to or objections to discrimination become a driver of competition and market standards. Pro-active steps taken by consumers themselves to enable self-help (e.g., avoiding automatically signing up to loyalty programs, setting browsers to reject cookies). Negative market reactions to pricing (e.g. Amazon’s differential pricing in 2000).(^{29})</td>
</tr>
</tbody>
</table>

*Source: Author’s own analysis.*

5.1. European Commission

On the question of whether EU competition law is fit-for-purpose in an AI environment, Commissioner for Competition Vestager has stated that:

‘... businesses also need to know that when they decide to use an automated system, they will be held responsible for what it does. So, they had better know how that system works.’

In terms of the attribution of liability for antitrust infringements, the European Commission treats an AI decision-maker in the same way as a human and a business cannot escape liability by simply attributing conduct to a machine.

It appears that the European Commission expects businesses to anticipate the possibility of a rogue AI decision-maker and they must take steps to limit its freedom by design. This policy and enforcement resembles the approach taken in relation to competition law compliance generally where a business is expected to take appropriate steps to train staff with a view to preventing anti-competitive conduct and cannot generally absolve itself from liability when those measures fail.

It is clear that the digital sector and the issues raised by data and AI in particular remain at the forefront of the European Commission’s policy agenda. In April 2019 the Commission published a report entitled Competition Policy for the digital era. The report makes interesting reading against the pending EU antitrust investigation into Amazon’s treatment of merchant data. The report identifies three key features of the digital economy: extreme returns relative to scale, network externalities, and the role of data. The writers of the report believe that the basic competition law framework under Articles 101 and 102 TFEU provides a sound basis for protecting competition in the digital economy. However, they note that the features of platforms, digital ecosystems and the data economy may need to be adapted when looking at the competition in the digital economy, such as self-learning algorithms: ‘...but machine learning means that the algorithms may themselves learn that co-ordination is the best way to maximise longer-term business objectives. In that case, no human agent has planned the co-ordination. Does that represent a breach of competition law? Does the law stretch to cover sins of omission as well as sins of commission: the failure to build in sufficient constraints on algorithmic behaviour to ensure that the algorithm does not learn to adopt anti-competitive outcomes? And what if constraints are built in but they are inadequately welcomed by the competition bars in Europe and the UK. In her first term of office, she can be credited for promoting greater awareness of competition issues, many making headline news including in high profile digital economy cases such as Google Shopping. The change of Competition Commissioner does not usually signal a dramatic shift in focus for DG Competition. If anything, Vestager’s re-appointment to the role means that those operating in the digital sector can expect continued scrutiny.

5.2. Competition and Markets Authority

The CMA has dealt with cases where AI has been a supporting factor in antitrust infringements. For example, on 1 August 2019, it fined Casio £3.7 million for infringing competition law by preventing online discounting of prices for its digital pianos and keyboards. The CMA found that Casio used new software that makes it easier to monitor online prices in real time and ensure compliance with its pricing policy. It also found that this meant that individual retailers had less incentive to discount for fear of being caught and potentially penalized. However, the CMA had evidence of an agreement (between Casio and each retailer) so could reconcile this case within the existing framework of liability under Chapter I of the Competition Act 1998.

On the issue of whether AI requires a rethink in the traditional notions of liability for antitrust infringements, the former CMA Chairman David Currie has expressed a more nuanced position than that expounded by the European Commission. He has questioned whether the legal tools currently available to the CMA are capable of tackling all the challenges presented by the rise of the algorithmic economy, such as self-learning algorithms:

Amazon’s CEO Jeff Bezos subsequently apologised for the differential pricing and promised that Amazon ‘never will test prices based on customer demographics’: see ‘Bezos calls Amazon experiment a mistake’ (28 September 2000), available at: https://www.bizjournals.com/seattle/stories/2000/09/25/daily01.html.

30 Bundeskartellamt 18th Conference on Competition Berlin (16 March 2017).

31 See, further, the European Commission’s guidance to businesses on compliance with competition law, available on its website at https://ec.europa.eu/competition/antitrust/compliance/index_en.html.


33 See, further, Competition Policy for the digital era (fn 32), ch 3.


35 Case 50655-2 Digital piano and digital keyboard sector: anti-competitive practices (1 August 2019).
designed, so that the very clever algorithm learns a way through the constraints? How far can the concept of human agency be stretched to cover these sorts of issues? I have suggested earlier that the competition tools at our disposal can tackle the competition issues that we face in the new digital world, but perhaps this last issue which I have touched on is one where this proposition is not true. (emphasis added)36

This may suggest that the question of attribution of liability (under the UK competition regime at least) is ripe for reassessment should developments in AI advance to such a state where the output of an AI system cannot be attributed to a human.

On the specific issue of whether algorithms may facilitate anti-competitive outcomes, the CMA has recently published an economic research paper on the role of pricing algorithms in online markets.37 This finds little evidence of companies using algorithms to show personalized prices, but they are sometimes used to change the order in which products are shown to shoppers.38 The CMA also found that algorithms can be used to help implement illegal price fixing and, under certain circumstances, could encourage a move to a coordinated equilibrium in markets already susceptible to coordination.39 However, it expresses a tentative view that in markets that are currently highly competitive it seems less likely that the use of data and algorithms would be so impactful that they could enable sustained collusion.40

5.3. United States

The United States has taken antitrust enforcement action in the context of online marketplace restrictions using algorithmic software. In 2015 the Department of Justice (‘DoJ’) filed a criminal complaint against David Topkins and his co-conspirators alleging that they had agreed to adopt specific pricing algorithms for their online posters and to coordinate price increases for a product sold on Amazon.41 Topkins is reported to have written code that instructed company algorithms to set prices in accordance with the agreement. At the time, the prosecutions raised speculation as to whether antitrust had indeed ‘come of age’ and was now ripe for re-assessment in the digital era. However, a closer examination of this case reveals that the DoJ had evidence of a clear anti-competitive agreement between the parties, albeit one that was implemented through the use of algorithmic software. In short, the agency could identify a human meeting of minds behind the use of those algorithms.

The rather limited antitrust enforcement practice against use of algorithms in the United States to date may be explained in part by the distinction between explicit collusion and tacit collusion. The former is generally prosecuted as a criminal offence, whereas the latter is in general lawful. The US agencies practically need evidence of or tantamount to communication between the parties that amounts to an agreement and this may not be straightforward to establish where AI systems are concerned.

5.4. Other jurisdictions

Beyond the EU and the United States antitrust authorities around the world have been asked to grapple with claims of infringement through or related to the use of algorithms. There is no consensus on how to deal with market manipulation that falls short of an anticompetitive agreement. While it is beyond the scope of this article to survey the comparative cases exhaustively an example will serve to illustrate that this is very much a live issue.

In 2018, the Competition Commission of India (‘CCI’) rejected42 a complaint against the ride-hailing platforms Uber and Ola that alleged that their use of algorithms artificially manipulated supply and demand contrary to section 3 of the Indian Competition Act 2002.43 The complainant alleged that the platforms acted as an unlawful hub and spoke to facilitate collusion between drivers to fix and artificially inflate their pricing using algorithmic software. The CCI found no such agreement among the drivers. It also distinguished the typical hub and spoke cartel arrangement which operates with a set of vertical agreements coordinated through a common counterparty and dismissed the claim that the platforms operated in the manner alleged. It also rejected a claim of unlawful resale price maintenance.

38 Pricing algorithms (fn 37), para 7.17.
39 Pricing algorithms (fn 37), para 8.6.
40 Pricing algorithms (fn 37), para 5.37.
41 Department of Justice press release No 15-421, Former E-Commerce Executive Charged with Price Fixing in the Antitrust Division’s First Online Marketplace Prosecution (6 April 2015).
43 Section 3 of the Indian Competition Act 2002 was informed by and is the practical equivalent under Indian competition law to Article 101 TFEU and Chapter I of the UK Competition Act 1998.
on the basis that there is no resale when the platforms match supply and demand. It found that applications-based taxi companies do not sell any service to drivers that is then resold to customers. Nor did it find evidence that prices negotiated individually would be lower than those established through algorithmic pricing.

6. (Initial) conclusions and areas for future research

AI has attracted significant antitrust interest, raising the question of whether the competition regimes as they stand are ready to address potentially anti-competitive outcomes arising from AI decisions. Although many issues arising with AI elide with the antitrust debate around Big data, AI and the use of algorithms raises its own rather specific issues.

The AI antitrust scholarship makes a bold claim that AI is an enabler of tacit collusion and could increase the scope for anti-competitive outcomes at even lower levels of concentration than associated with antitrust orthodoxy. However, even the brief examination of these claims in this article has unearthed alternative hypotheses which need to be fully tested before the theory can be incorporated in policy and legal environments without running the risk of being counter-productive.

The following areas would merit attention as topics for further research and analysis:

- Analysis of the effects of algorithms on incentives for tacit collusion and their destabilizing effects including in markets which are not already prone to tacit collusion. In particular, this involves understanding how robust the predictions in the AI literature are to their assumptions (e.g. algorithmic heterogeneity, larger number of sellers etc).
- Whether there might be alternative outcomes which present competition or other concerns but which are not caught within traditional antitrust paradigms (e.g. data capture, data extraction and co-operation between super-platforms and applications developers).
- Understanding rational and harmful price transparency and whether and when particular consumer outcomes are an appropriate case for antitrust intervention. This accepts that consumers make bad decisions even in competitive markets and that instances of consumers making bad decisions caused by algorithmic pricing may not be an appropriate case for antitrust intervention.
- Understanding countervailing AI strategies by buyers under a range of assumptions, including across B2C and B2B markets.
- Understanding the appropriate boundaries of liability and the circumstances in which an algorithm may be traced back to its owners and the extent to which those owners should be subject to (vicarious) antitrust responsibilities and enforcement.
- Understanding the main goals of antitrust which are impacted by AI. The current resistance on the part of regulators in Europe and the United States to regulate wealth transfers between AI sellers and buyers could place limits on the application of antitrust to consumer exploitation such as through data extraction. Ezrachi and Stucke have, however, presented an additional gloss in the idea that virtual competition increases the ‘dead weight loss by increasing distrust’.44 Further examination is needed as to whether presenting the social costs of algorithms within a paradigm of (mis)trust provides an appropriate analytical construct that is capable of real-world application so as to legitimize antitrust interventions within a coherent welfare-based model.
- Where personal data is shared with another market participant, the extent to which such data sharing would involve sharing of competitively sensitive information with a competitor and how such sharing may be compatible with antitrust law.45

A technological understanding of algorithms and how they operate is critical. For now, at least, it seems that the antitrust authorities will typically be able to find evidence of human involvement where machines or algorithms are identified as facilitators of anti-competitive conduct. However, the fact remains that technology will probably evolve to such a point where this situation does not always hold true. Ultimately enforcers, practitioners and businesses will have to confront the question of liability for the decisions or output of machine learning which are increasingly distanced from human intervention and which call into question traditional notions of antitrust liability.

44 Ezrachi and Stucke (fn 1), p 242.
45 A current debate is whether there is an enforcement gap in mergers in relation to lost potential competition in such situations and in Big data scenarios more generally. This issue of whether AI in the hands of a limited number of data controllers is adequately addressed under merger control was not explored in this article.