Canadian Journal of Law and Technology

Volume 16 | Number 2 Article 7

1-1-2016

Corporate Criminal Liability for Algorithmic Price Fixing in Canada

Theodore Milosevic
Student-at-Law, Blake, Cassels & Graydon LLP, Toronto

Corporate Criminal Liability for Algorithmic Price-Fixing in Canada

Theo Milosevic*

INTRODUCTION

The use of computerized algorithms is increasingly common in the modern business environment.[1] An algorithm can be defined as "a set of mathematical instructions or rules that, especially if given to a computer, will help to calculate an answer to a problem."[2] As noted in this definition, algorithms are particularly powerful tools when combined with computing power.

The proliferation of computerized algorithms in business settings has occasionally led to unintended and injurious outcomes. This is perhaps most notable in relation to the algorithmic trading of securities. The 2010 "Flash Crash" of the United States (U.S.) financial markets, during which key markets lost and then regained over a trillion dollars in value over the span of 36 minutes, was caused, at least in part, by the intentional manipulation of algorithmic trading processes.[3] Another example is that of Knight Capital, a financial services firm, which, in 2012, lost approximately USD 440 million in just 45 minutes due to a faulty algorithm.[4] Unsurprisingly, securities regulators stand at the forefront of regulating algorithms, with U.S. and European (E.U.) agencies both developing policies in this regard.[5,6] Complying with regulations aimed at algorithms will be a novel challenge for the financial trading industry.

---

* Theo Milosevic is a Student-at-Law at Blake, Cassels & Graydon LLP in Toronto. Theo would like to thank Mr. Kenneth Jull for his instruction in the course "Financial Crimes and Corporate Compliance" at the University of Toronto Faculty of Law, which led to the development of this paper.

1 H James Wilson, Allan Alter & Prashant Shukla, "Companies Are Reimagining Business Processes with Algorithms", *Harvard Business Review* (8 February 2016), online: < https://hbr.org/2016/02/companies-are-reimagining-business-processes-with-algorithms > .

2 *Cambridge Advanced Learner's Dictionary*, 4th ed, sub verbo "algorithm."

3 Lindsay Whipp & Kara Scannell, "'Flash-crash' trader Navinder Sarao pleads guilty to spoofing," *Financial Times* (9 November 2016), online: < www.ft.com/content/a321031a-a6cb-11e6-8898-79a99e2a4de6 > .

4 Nathaniel Popper, "Knight Capital Says Trading Glitch Cost It $440 Million", *The New York Times* (2 August 2012), online: < dealbook.nytimes.com/2012/08/02/knight-capital-says-trading-mishap-cost-it-440-million/ > .

5 Lisa Lambert, "SEC working toward algorithmic trading rule", *Reuters* (19 February 2016), online: < www.reuters.com/article/us-sec-trading-algorithmic-idUSKCN0VS2MW > .

6 Danny Busch, "MiFID II: Regulating High Frequency Trading, Other Forms of Algorithmic Trading and Direct Electronic Market Access," (12 July 2016) *University of*

However, the use of computerized algorithms also carries substantial compliance-related implications for companies outside of the trading field. This is particularly notable in regard to the intersection between competition law and the algorithmic pricing used in online retail. This paper examines the issue of corporate criminal liability in Canada for potential violations of price-fixing laws resulting from the use of algorithmic pricing. The central argument of the paper is that it is possible to both legally establish and theoretically justify criminal punishment in situations where humans have arranged a price-fixing agreement and use pricing algorithms as the tool to carry out the agreement. However, in situations where algorithmic price-fixing is an unintended outcome that results from the semi-autonomous or autonomous development of a pricing algorithm, the imposition of criminal liability may be difficult to legally establish and to justify. As such, I argue that a civil provision for regulating price-fixing is the appropriate tool to address algorithmic price-fixing that results absent explicit intent or direction by the human designer. The lens of analysis for these arguments is Canadian price-fixing legislation in their current form.

The paper is structured in five parts. Part I provides an overview of algorithms as a concept and tool by briefly examining the range of uses for algorithms in modern businesses. Part II explores the interconnection between pricing algorithms and competition law, drawing on empirical and theoretical examples in the process. Third, the paper examines corporate criminal liability under the *Criminal Code* of Canada[7] and s. 45 of the *Competition Act*[8] (the "*Act*"), and assesses whether and how the use of algorithms complicates the assessment of corporate criminal liability. Fourth, the paper shifts to the question of how to justify criminal punishment for algorithmic price-fixing under utilitarian and normative theories of punishment. The paper concludes by summarizing the argument that the use of criminal price-fixing provisions should be limited to instances in which humans deliberately arrange a price-fixing agreement that uses pricing algorithms as the tool to carry out the agreement.

OVERVIEW OF COMPUTERIZED ALGORITHMS

At the most basic level, algorithms are a simple concept. An algorithm is a systematic set of steps that one uses to reach a desired outcome. Algorithms are used in many day-to-day aspects of society, and the history of algorithms can be traced to fields such as food preparation, grammar, and medicine.[9] The field of mathematics is most closely linked to the development of algorithms as a formal tool and a general concept, and, upon the development of computing technology,

---

Oxford Business Law Blog, online: <www.law.ox.ac.uk/business-law-blog/blog/2016/07/mifid-ii-regulating-high-frequency-trading-other-forms-algorithmic>.

7 *Criminal Code*, R.S.C. 1985, c. C-46.

8 *Competition Act*, R.S.C. 1985, c. C-34, s. 45.

9 Jean-Luc Chabert & Evelyne Barbin, eds, *A History of Algorithms*, 1st ed (Berlin: Springer, 1999) at 1-7.

the ways in which algorithms were used in mathematics quickly gained traction in the field of computer science.[10]

Algorithms in computer science vary in terms of specific purpose but are generally based around the same general principle, whereby a defined set of input data is subjected to one or multiple specific procedures in order to produce outputs which are intended to solve a particular problem or reach a desired end point. Computerized algorithms are typically able to accomplish that which would not be possible manually due to the processing power and interconnectivity of modern computers. These factors allow computerized algorithms to access a greater range of data than would be accessible by humans, and to process this vast data and enact changes in the algorithmic output faster than humans are able to.[11]

At focus in this paper are algorithmic pricing systems used by online retailers. Online retailers use algorithms with the goal of setting the "optimal" price relative to market dynamics. Computerized pricing algorithms offer significant advantages over manual price-setting as they can access and process more data than humans and can automatically reflect pricing alterations faster and with more frequency than would be possible manually.[12] These pricing algorithms vary, as they can be used to either assign a good or service an initial price, or to continuously update the price of a given good or service. In both of these scenarios, the algorithm is designed to achieve a goal such as setting a price which matches demand exactly, or setting a price that is in some way competitive relative to other sellers in the market.[13] The key aspects of pricing algorithms are the factors employed to determine price levels, such as competitor pricing, market trends, demand, inventory, and individualized consumer information such as purchasing history.[14] Pricing algorithms have become relatively ubiquitous in e-commerce, and are particularly pervasive in large online marketplaces such as Amazon Marketplace, which bring together many retailers selling similar or identical goods.[15]

There are two further points of interest in regard to the use of computerized algorithms. First, these algorithms are sometimes structured as iterative processes which are able to "learn" by autonomously incorporating new data

---

[10] *Ibid.*

[11] Steve Lohr, "Google Schools Its Algorithm", *The New York Times* (5 March 2016), online: < www.nytimes.com/2011/03/06/weekinreview/06lohr.html > .

[12] Ariel Ezrachi & Maurice E. Stucke, "Artificial Intelligence and Collusion: When Computers Inhibit Competition," (2016) The University of Oxford Centre for Competition Law and Policy, working paper No. CCLP (L) 40.

[13] *Ibid.*

[14] Le Chen, Alan Mislove & Christo Wilson, "An Empirical Analysis of Algorithmic Pricing on Amazon Marketplace," in *Proceedings of the 25th International Conference on World Wide Web* (Geneva: International World Wide Web Conference Steering Committee, 2016.

[15] *Ibid.*

and weighing data differently based on the success of results or shifting market dynamics.[16] For example, homestay platform AirBnB uses a pricing algorithm that bases prices off of the key characteristics of each listed property, such as number of bedrooms, location, and amenities, and market dynamics, such as seasonal patterns and demand. However, this model is not static. It is continuously judging its price-setting against actual outcomes, meaning it gathers information regarding whether there is a shortage or excess of demand for a particular property at a given price level. It subsequently incorporates that information into the model and adjusts its weighting of pricing factors to try to achieve price levels that reduce inefficiencies associated with excesses or shortages in demand.[17] This dynamic process is called "machine-learning" and creates a system whereby the pricing algorithm is autonomously changing and growing.

The second point is that the increasing prevalence of algorithms means that they frequently interact. For example, a pricing algorithm used by an online retailer may incorporate competitor pricing, which could itself have been determined by pricing algorithms based on competitor pricing. This interaction between algorithms creates the possibility for a number of unintended and potentially harmful consequences such as feedback loops between two closely linked algorithms. This was the case in 2011, when the price of a book sold by two retailers on Amazon rose from under USD 100 to over USD 23 million in less than a week. One observer attributed this sudden increase to each retailer designing their pricing algorithm to price the book predominantly as a function of the other retailer's price, creating a system whereby a slight variation in the price of one retailer's book caused both algorithms to enter into a theoretically endless cycle of price escalation without the knowledge of either retailer.[18] It is massively difficult to predict how, if, and when phenomena of this nature will occur, but the potential for such problems underscores the compliance-related issues facing the use of computerized algorithms.

---

[16] For a comprehensive overview see: Ashwin Ittoo & Nicolas Petit, "Algorithmic Pricing Agents and Tacit Collusion: A Technological Perspective," (2017) [unpublished, online at SSRN: < papers.ssrn.com/sol3/papers.cfm?abstract_id = 3046405 >].

[17] Dan Hill, "The Secret of Airbnb's Pricing Algorithm," *IEEE Spectrum* (20 August 2015), online: < spectrum.ieee.org/computing/software/the-secret-of-airbnbs-pricing-algorithm > .

[18] John D. Sutter, "Amazon seller lists book at $23,698,655.93 – plus shipping", *CNN* (25 April 2011), online: < www.cnn.com/2011/TECH/web/04/25/amazon.price.algorithm/ > . See also Canada, Competition Bureau Draft Discussion Paper, "Big Data and Innovation: Implications for competition policy in Canada," (2017), online: < www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/vwapj/Big-Data-e.pdf/$file/Big-Data-e.pdf > , in which the Competition Bureau uses this example to illustrate the potential for 'big data' to impact a market.

PRICING ALGORITHMS AND COMPETITION LAW

A growing amount of regulatory focus[19], jurisprudence[20], scholarly thought,[21] and media attention[22] is focused on the interrelation between the use of algorithms and price-fixing.

Price-fixing, which is closely linked to the concepts of cartels, collusion, and conspiracy, is, in many jurisdictions, a criminal offence directed at preventing "agreements between two or more persons to prevent or unduly lessen competition or to unreasonably enhance the price of a product."[23] The precise nature of price-fixing offences varies by jurisdiction, but, at the broadest level, they generally require intent by multiple parties to control the price of a product.

Marketplace and competition regulators have explicitly focused on the potential intersection between algorithmic pricing and price-fixing since at least the beginning of 2017. This regulatory focus is evident in a June 2017 roundtable on "Algorithms and Collusion," held by the Organization for Economic Co-operation and Development (OECD).[24]

Existing academic work[25] and litigation[26] related to algorithms and price-fixing laws focuses on pricing algorithms, such as those used in the Amazon

---

[19] OECD, *Algorithms and Collusion—Note from the European Union*, Doc. No. DAF/COMP/WD (2017) 12 (2017) [EU OECD Paper; OECD Financial and Enterprise Affairs Competition Committee, *Algorithms and Collusion—Note by the United States,* Doc. No. DAF/COMP/WD (2017)41 (2017) [US OECD Paper]; OECD Financial and Enterprise Affairs Competition Committee, *Algorithms and Collusion—Background Note by the Secretariat*, Doc. No. DAF/COMP/ (2017)4 (2017).

[20] See e.g. *Meyer v. Uber Technologies Inc.* , No. 16-2750 (US 2nd Ct, 2017) [*Meyer*]; *United States v. Topkins* (2015) CR 15-00201 WHO, online < www.justice.gov/atr/case-document/file/628891/download > [*Topkins*].

[21] Ezrachi & Stucke, "Artificial Intelligence," *supra* note 12; Joseph E Harrington Jr., "Developing Competition Law for Collusion by Autonomous Price-Setting Agents," (2017), [unpublished, online at SSRN: < ssrn.com/abstract = 3037818 >]; Ariel Ezrachi & Maurice E Stucke, "Two Artificial Neural Networks Meet in an Online Hub and Change the Future (Of Competition, Market Dynamics and Society)" (July 2017), [unpublished, online at SSRN: < papers.ssrn.com/sol3/papers.cfm?abstract_id = 2949434 >]; Ittoo & Petit, *supra* note 16; Salil K. Mehra, "US v. Topkins: can price fixing be based on algorithms?" (2016) 7:7 J Eur Competition Law & Practice 470; Salil K. Mehra, "Antitrust and the Robo-Seller: Competition in the Time of Algorithms" (2016) 100 Minn L Rev 1323; Andreas Heinemann & Aleksandra Gebicka, "Can Computers Form Cartels? About the Need for European Institutions to Revise the Concentration Doctrine in the Information Age" (2016) 7:7 J Eur Competition Law & Practice 431.

[22] Jill Priluck, "When Bots Collude," *The New Yorker* (25 April 2015), online: < www.newyorker.com/business/currency/when-bots-collude > ; David Lynch, "Poli-Policing the digital cartels", *Financial Times* (8 January 2017), online: < www.ft.com/content/9de9fb80-cd23-11e6-864f-20dcb35cede2 > .

[23] Competition Bureau, "Price-fixing" (22 February 2018), online: < www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/h_00112.html > .

[24] See *supra* note 19 for background papers submitted as part of the OECD roundtable.

Marketplace, and points towards a spectrum of ways in which the use of algorithms can potentially lead to violations of price-fixing laws. At one end of this spectrum — likely the clearer end in terms of assessing corporate liability — lie firms which intentionally arrange a traditional conspiracy agreement but use coordinated algorithmic price-setting as the tool to carry out the agreement. At the other, more opaque, end of this theoretical spectrum lie situations in which some sort of coordinated price-fixing may occur due solely to the autonomous decision-making of price-setting algorithms. The following section will develop a conceptual framework for understanding the ways in which algorithms can relate to price-fixing.

CONCEPTUALIZING THE RELATIONSHIP BETWEEN ALGORITHMIC PRICING AND PRICE-FIXING

In a simple corporate structure of one company without parents, subsidies, or affiliates, one can consider the relationship between algorithmic pricing and price-fixing to fall along a spectrum of human control. On one end of this spectrum, humans exercise significant control over the price-fixing function of pricing algorithms. On the other, the use of largely autonomous pricing algorithms may lead to outcomes which resemble traditional price-fixing.

The clear end of this spectrum is the use of algorithmic pricing by humans as a tool for price-fixing. This has been termed the "messenger"[27] category of collusion, and conforms well with traditional notions of liability for price-fixing. The first North American price-fixing charge related to the use of algorithmic pricing falls under this category. In 2015, the United States Department of Justice Antitrust Division charged California resident David Topkins with price-fixing for his conduct as a director of an e-commerce company selling posters between 2013 and 2014.[28] Topkins, who subsequently pled guilty, and co-conspirators from competitor companies agreed to fix prices of certain posters sold on Amazon Marketplace, and adopted "specific pricing algorithms for the agreed upon posters with the goal of coordinating changes to their respective prices."[29] In response to the charge, Bill Baer, Assistant Attorney General of the U.S. Department of Justice Antitrust Division, said, "[w]e will not tolerate anticompetitive conduct, whether it occurs in a smoke-filled room or over the Internet using complex pricing algorithms."[30]

---

[25] See *supra* note 21.

[26] See *supra* note 20.

[27] Ezrachi & Stucke, "Artificial Intelligence," *supra* note 12 at 10.

[28] *Topkins, supra* note 20.

[29] *Ibid* at para 4.

[30] United States Department of Justice, Press Release, 15-421, "Former E-Commerce Executive Charged with Price Fixing in the Antitrust Division's First Online Marketplace Prosecution" (11 February 2016), online: <www.justice.gov/opa/pr/former-e-

On the other end of the spectrum are situations in which pricing algorithms, in pursuit of a human-determined end goal, leverage machine learning to autonomously determine the best means of achieving this target. This has been termed the "autonomous machines"[31] scenario, and creates the potential for algorithms working alone or in concert to determine that some form of coordinated price-fixing or market sharing is the best strategy to achieve their intended goal. While the evidence of any such activity is limited, anecdotal, and somewhat speculative,[32] machine learning capacity, interconnection between algorithms, and the present pace of technological development brings it into the realm of possibility.[33] It is thought that such a situation is most likely to arise in a stable and concentrated market "involving homogenous products where the algorithms can monitor to a sufficient degree the pricing and other keys terms of sale."[34]

This situation would pose a significant dilemma for regulators and policy-makers as it would create outcomes similar to traditional price-fixing, but absent any formal intent or agreement which problematizes notions of liability.

In between these two ends of the spectrum is a gray-zone termed the "predictable agent"[35] scenario, wherein industry dynamics lead competitors to develop pricing algorithms that they know will likely lead to shifts in market structure. For example, an online retailer, possessing the intent to shift market dynamics in terms of supply or price, could design a pricing algorithm that they know will interact with competitors' pricing schemes to achieve such a goal. These situations are characterized by a lack of explicit agreements between competitors, and recent academic work has argued that pricing algorithms are particularly well-designed to facilitate tacit collusion of this nature.[36]

Pricing algorithms can also run up against price-fixing laws in "hub-and-spoke" scenarios. In this form of collusion, a "hub" firm arranges vertical restraints with a number of the downstream or upstream "spoke" firms with which it interacts. These spoke firms collectively agree to adhere to the vertical restraints of the hub firm. Illegality under price-fixing laws may arise if a "hub-and-spoke" arrangement artificially controls the price of a product. In terms of algorithmic pricing, potential problems arise if a hub firm coordinates or is used to coordinate the use of an identical pricing algorithm by the spoke firms.

---

commerce-executive-charged-price-fixing-antitrust-divisions-first-online-marketplace > .

31 Ezrachi & Stucke, "Artificial Intelligence," *supra* note 12 at 22.

32 See Ezrachi & Stucke, "Neural Networks," *supra* note 21 at 8-12 for a discussion of possible real-world examples, and a more critical view in Ittoo & Petit, *supra* note 21 at 2-3.

33 Ittoo & Petit, *supra* note 21 at 13.

34 Ezrachi & Stucke, "Neural Networks," *supra* note 21 at 4.

35 *Ibid* at 16.

36 *Ibid*.

A complex example of this hub-and-spoke scenario is currently subject to litigation in the United States. In January 2016, an American man filed a civil lawsuit against the founder of car service Uber, which serves to connect users seeking transportation to drivers willing to provide transportation at a fee.[37] The civil action alleges that Uber is engaging in anti-competitive price-fixing by requiring the drivers operating as part of their platform to use the same pricing algorithm to determine fares, instead of allowing drivers to compete on price.[38] In a hub-and-spoke conceptualization of this scenario, the "hub" is Uber, the vertical agreements are the requirement to use Uber's pricing algorithm, and there is an implied horizontal agreement between the "spoke" Uber drivers to use the pricing algorithm.[39]

The spectrum of human control over algorithmic pricing is depicted in Figure 1.

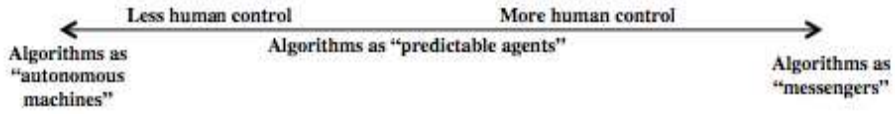

Figure 1: Human Control and Algorithmic Scenarios

CORPORATE CRIMINAL LIABILITY UNDER CANADIAN PRICE-FIXING LAWS

This section of the paper intends to answer the following question: assuming that there is evidence of coordination between competitors to achieve price controls through the use of pricing algorithms, in what circumstances will it be possible to establish corporate criminal liability for such coordination under Canadian price-fixing laws? The conclusions of this analysis are summarized at the end of this section.

In Canada, price-fixing is a criminal offence outlined in s. 45 of the *Competition Act,* which reads as follows:

> **45** (1) Every person commits an offence who, with a competitor of that person with respect to a product, conspires, agrees or arranges
>
> (a) to fix, maintain, increase or control the price for the supply of the product;
>
> (b) to allocate sales, territories, customers or markets for the production or supply of the product; or

---

[37] *Meyer, supra* note 20; Nicholas Passaro, "How Meyer v. Kalanick Could Determine How Uber and the Sharing Economy Fit into Antitrust Law," 6:2 Mich Bus & Entrepreneurial L Rev [forthcoming in 2018.

[38] *Meyer*, *supra* note 20.

[39] Passaro, *supra* note 37.

> (c) to fix, maintain, control, prevent, lessen or eliminate the production or supply of the product.[40]

The penalties under s. 45 are up to 14 years' imprisonment or a fine not exceeding CAD 25 million, or both. The Act also outlines a defence which reads:

> **45** (4) No person shall be convicted of an offence under subsection (1) in respect of a conspiracy, agreement or arrangement that would otherwise contravene that subsection if
>
> (a) that person establishes, on a balance of probabilities, that
>
> (i) it is ancillary to a broader or separate agreement or arrangement that includes the same parties, and
>
> (ii) it is directly related to, and reasonably necessary for giving effect to, the objective of that broader or separate agreement or arrangement; and
>
> (b) the broader or separate agreement or arrangement, considered alone, does not contravene that subsection.[41]

There is also a statutory exemption if the agreement is only entered into by firms which are "in respect of every one of the others, an affiliate."[42]

There are three predominant factors to consider in assessing corporate criminal liability for price-fixing in Canada. The following analysis considers these factors in turn, and addresses their relation to the use of pricing algorithms.

1. Corporate *actus reus*

The *actus reus* component of s. 45 requires that a person "conspires, agrees, or arranges" with a competitor to control the price of a product, control the quantity of a product that is produced or supplied, or to "allocate sales, territories, customers or markets for the production or supply" of a product. [43] A corporation can become a party to the offence if any of its "senior officers,"[44] acting with the intent to benefit the organization and within the scope of their authority, personally breaches s. 45, directs the work of other representatives of the corporation with the effect of breaching s. 45, or, while "knowing that a representative of the organization is or is about to be a party to the offence, does not take all reasonable measures to stop them from being a party to the offence."[45]

As such, the *actus reus* component of establishing corporate criminal liability for a s. 45 offence is established if a senior officer of the corporation acts or fails to act in one of the ways enumerated above.

---

[40] *Competition Act, supra* note 8, s. 45(1).

[41] *Ibid,* s. 45(4).

[42] *Ibid,* s. 45(6); see *contra* notes 62-65 for a discussion of which personnel constitute "senior officers."

[43] *Ibid,* s. 45(1).

[44] *Criminal Code, supra* note 7, s. 22.2.

[45] *Ibid.*

The *actus reus* requirement is a straightforward consideration in the "messenger" situation, whereby two or more corporations design and implement algorithms as tools to achieve a price-fixing agreement. In these circumstances, there is a clear and explicit agreement between corporate representatives in regard to using pricing algorithms to carry out price-fixing. For similar reasons, establishing the *actus reus* may be straightforward in some "hub-and-spoke" scenarios although, as in the Uber example outlined above, some hub-and-spoke scenarios may involve additional complexities.

The *actus reus* requirement is more difficult to establish in the autonomous machine and predictable agent scenarios, in which algorithms may form a price-fixing arrangement without direct human intervention.

One line of argument asserts that there is no conspiracy, agreement, or arrangement in such circumstances because machines are incapable of forming an explicit agreement or arrangement in the way that humans are able to. Under this line of thinking, any form of coordination between pricing algorithms would, at most, fall under the category of tacit collusion, whereby competitors somehow coordinate pricing without any explicit arrangements, or conscious parallelism, a pricing phenomenon in oligopolistic markets whereby competitors recognize the advantages of coordinated pricing without any explicit agreement.[46]

The Canadian Competition Bureau's policy on pursuing tacit collusion under s. 45 is unclear, while Canadian courts have found that instances of conscious parallelism does not fall under the purview of s. 45.[47] In regard to s. 45, the Bureau's 2009 guidelines on enforcing the provision indicate that the Bureau will consider tacit arrangements,[48] while the 2001 guidelines state that "the ability of a group of firms to coordinate actions without entering into an explicit agreement can be addressed under the abuse provisions"[49] in ss. 78 and 79 of the *Act*.[50]

If one adopts the viewpoint that algorithms are able to form explicit agreements without human intervention,[51] there is the residual problem of connecting the conduct of these pricing algorithms to the corporation. This same issue has been dealt with in the field of electronic contract formation, in which advanced programs may bind a legal person to a contract.[52] According to law

---

[46] WT Stanbury & GB Reschenthaler, "Oligopoly and Conscious Parallelism: Theory, Policy and the Canadian Cases" (1977) 15:3 Osgoode Hall LJ 617.

[47] Michael Trebilcock, Edward M Iacobucci & Ralph A Winter, *The Law and Economics of Canadian Competition Policy* (Toronto: University of Toronto Press, 2002) at 112.

[48] Canada, Competition Bureau, *Competitor Collaboration Guidelines,* December 2009 update (Gatineau: Competition Bureau, 2009) at 6.

[49] Calvin S Goldman & John D Bodrug, eds, *Competition Law of Canada*, 1st ed (Huntington, NY: Juris, 1996), at 9-103.

[50] *Competition Act, supra* note 8, ss. 78-79.

[51] See *contra* notes 78-82: EU regulators are considering the possibility of interpreting their competition laws such that the term "communication" may be used to cover interactions between algorithms.

and technology scholar Professor Ian Kerr, a prominent approach, as found in Canada's *Uniform Electronic Commerce Act*[53] and the *UNCITRAL Model Law on Electronic Commerce*[54] is to "treat the operations of the automated agent as a mere extension of the actions of the human being who initiated its use."[55] This can be referred to as the "attribution rule," and is a rule of absolute liability for the originating human, as opposed to one based in principles of authority and agency.[56] Using the attribution rule in this way, the conduct of the pricing algorithm could be taken to fulfill the *actus reus* of a corporate representative. David C. Vladeck summarizes the logic behind this viewpoint as follows:

> [t]he human hand defines, guides, and ultimately controls the process, either directly or because of the capacity to override the machine and seize control . . . Where the hand of human involvement in machine decision-making is so evident, there is no need to reexamine liability rules. Any human (or corporate entity that has the power to do things that humans do, enter into contracts, hire workers, and so forth) that has a role in the development of the machine and helps map out its decision-making is potentially responsible for wrongful acts—negligent or intentional—committed by, or involving, the machine. The reason, of course, is that these machines, notwithstanding their sophistication, have no attribute of legal personhood. They are agents or instruments of other entities that have legal capacity as individuals, corporations, or other legal "persons" that may be held accountable under the law for their actions.[57]

However, as noted by Professor Kerr, adopting such a hardline approach "could lead to unjust results in situations where a transaction generated by the intelligent agent is unintended, unforeseen or unauthorized by its human originator."[58]

Of further note is some theoretical discussion in academic literature regarding imbuing artificially intelligent machines or programs with legal personhood.[59] While this remains only an abstract possibility, it could be

---

[52] Ian Kerr, "Ensuring the Success of Contract Formation in Agent-Mediated Electronic Commerce" (2001) 1 Electronic Commerce Research Journal 183 at 191-193.

[53] Uniform Law Conference of Canada, *Uniform Electronic Commerce Act* (Winnipeg: Uniform Law Conference of Canada, 1998).

[54] UN Commission on International Trade Law, *UNCITRAL Model Law on Electronic Commerce* (Vienna: United Nations, 1996).

[55] Kerr, *supra* note 52 at 191.

[56] *Ibid.*

[57] David C. Vladeck, "Machines Without Principals: Liability Rules and Artificial Intelligence" (2014) 89:1 Wash L Rev 117 at 120-121.

[58] Kerr, *supra* note 52 at 192.

[59] See Kerr, *supra* note 52 at 189; Lawrence B. Solum, "Legal Personhood for Artificial Intelligences" (1992) 70:4 NC L Rev.

another way of attaching the *actus reus* of algorthimic price-fixing to a corporation.

2. Corporate *mens rea*

Establishing *mens rea* is the key complicating factor in terms of assessing corporate criminal liability for price-fixing related to the use of algorithmic pricing. As corporations are not natural persons, the *mens rea* requirement is met through the *mens rea* of a corporation's "senior officers" as outlined in s. 22.2 of the *Criminal Code*.[60]

The term "senior officer" is a very context-specific concept, which refers to any representative of an organization "who plays an important role in the establishment of an organization's policies or is responsible for managing an important aspect of the organization's activities and, in the case of a body corporate, includes a director, its chief executive officer and its chief financial officer."[61] A senior officer can bind its corporation to a criminal offence if, "with the intent at least in part to benefit the organization,"[62] he or she,

> (a) acting within the scope of their authority, is a party to the offence;
> (b) having the mental state required to be a party to the offence and acting within the scope of their authority, directs the work of other representatives of the organization so that they do the act or make the omission specified in the offence; or
> (c) knowing that a representative of the organization is or is about to be a party to the offence, does not take all reasonable measures to stop them from being a party to the offence.[63]

This approach casts a broad and somewhat opaque net of criminal liability over corporations in Canada.

While the jurisprudence regarding who qualifies as a "senior officer" is nascent and quite limited, some insight can be gained from the case of *R. c. Pétroles Global*[64] in which Justice Tôth of the Quebec Superior Court elaborated on how courts should approach the senior officer concept. The critical elements of Justice Tôth's ruling are that assessing who is a senior officer requires a fully contextualized analysis of the organization in question and the individual's role therein,[65] that senior officers are not delineated solely by a specific title,[66] and

---

60 *Criminal Code, supra* note 7, s. 22.2.

61 *Ibid,* s. 2.

62 *Ibid,* s. 22.2.

63 *Ibid.*

64 *R. c. Pétroles Global inc*, 2015 QCCS 1618, 2015 CarswellQue 3514 (Que. Sup. Ct.) [*Pétroles Global*].

65 Todd L. Archibald, Kenneth E. Jull & Kent W. Roach, *Regulatory and Corporate Liability: From Due Diligence to Risk Management*, 2nd ed (Toronto: Thomson Reuters, 2016) at 5-15.

66 *Ibid.*

that one can still be a senior officer even if their decisions must be approved by another officer of the organization.[67] Justice Tôth's ruling confirmed that corporate criminal liability in Canada has been expanded "outside the boardroom and onto the plant floor"[68] under the senior officer doctrine.

Given this extension of liability beyond only the highest levels of corporate management, one immediate question in terms of assessing corporate criminal liability for algorithmic price-fixing is whether those individuals designing pricing algorithms can be deemed senior officers. This is clearly a context-dependent question which will turn on the nature of the business, the corporate structure, the size of the corporation, and the specific staffing arrangements within the organization. However, in an organization engaging primarily in electronic commerce, one could make a strong argument that those designing the structure of pricing algorithms are responsible for "managing an important aspect of the organization's activities" as is required by the *Criminal Code*. Archibald, Jull, and Roach state that senior officers should be thought of as "those employees who are empowered to make business decision that involve the taking of reasonable risks."[69] Determining how goods or services are priced seems like a business decision that involves the taking of reasonable risks, and, at least in some circumstances, the pricing classification of the algorithm designer as a senior officer. As per *Pétroles Global,* the fact that a higher level of management may need to approve a pricing algorithm does not preclude the algorithm designer from being classified as a senior officer.

With that in mind, the focus then shifts to examining the interconnection between liability under s. 22.2 of the *Criminal Code* and the aforementioned scenarios in which the use of pricing algorithms leads to violations of s. 45 of the *Competition Act*. Section 22.2(a) is well-positioned to capture the messenger scenario, assuming that a senior officer has arranged to use pricing algorithms as a price-fixing tool with a competitor in order to benefit the corporation. This also applies to the hub-and-spoke scenario.

The senior officer in either situation could be executive management, but, as discussed above, the intent of an individual or individuals primarily responsible for designing pricing algorithms may also be sufficient to establish corporate criminal liability. Section 22.2(b) will also capture situations in which a senior officer directs a subordinate, who may not be properly considered a senior officer, to design or implement a pricing algorithm with the intent to commit price-fixing under the *Competition Act*.

The *mens rea* requirement may also be fulfilled in the predictable agent situation. The predictable agent scenario is marked by human intent to control prices absent any formal agreement. As previously discussed, establishing the

---

[67] *Ibid* at 5-19.

[68] *Ibid* at 5-14.

[69] *Ibid* at 5-16.

corporate *actus reus* will likely be the major challenge in regard to the predictable agent scenario due to the lack of explicit agreement between competitors.

Finally, establishing the requisite *mens rea* in the "autonomous machine" scenario will be difficult. Given the lack of human intent from the outset, activity in such a scenario may only be captured under the *Act* if the algorithm designer becomes aware that the pricing algorithm has developed some sort of price-fixing scheme in coordination with competitor algorithms and does nothing to stop this. This situation would potentially fall under s. 22.2(c), although this argument would still require the classification of the pricing algorithm as a "representative" of the organization. The *Criminal Code* defines a "representative" as a "director, partner, employee, member, agent or contractor of the organization," and, while this appears to indicate that a representative must be a legal person, that conclusion is not explicitly indicated in the text.[70]

The term "electronic agent" has been employed in the field of electronic contract formation, but this term does not refer to a typical agency relationship.[71] The notes to Canada's model law in this area are clear that "an electronic agent is a tool, not an agent in law."[72] Under such a conceptualization, it would be difficult to make the argument that algorithms are in fact standalone representatives of the organization.

RELEVANT EXEMPTIONS AND DEFENCES

As outlined above, s. 45(4) of the *Act* offers an "ancillary restraints" defence, which holds that an agreement that would otherwise fall under s. 45 does not result in an offence if it is ancillary to a broader separate arrangement, and reasonably necessary for giving effect to that broader agreement. This defence is available to all potential violations of s. 45.

Section 45(5) provides a narrower defence available to price-fixing agreements that relate only to the export of products from Canada.

Section 45(6) carves out an exemption for price-fixing arrangements entered into by organizations which are "in respect of every one of the others, an affiliate."[73] This includes all common subsidiaries of one parent corporation, as well as the relationship between parent and subsidiary companies.[74] Situations in which a controlling hub corporation employs coordinated pricing algorithms for spoke organizations under its control will be exempted as per s. 45(6).

Section 22.2(c) of the *Criminal Code* offers another possible avenue for negating liability. While this particular paragraph has not been subject to significant litigation, it appears from a common reading that the corporation will

---

70 *Criminal Code, supra* note 7, s. 2.

71 Kerr, *supra* note 52 at 191.

72 *Ibid.*

73 *Competition Act, supra* note 8, s. 45(6).

74 *Ibid,* s. 2.

not be liable if a senior officer is not a party to the offence, has not directed a representative to commit the offence, and takes "all reasonable steps" to stop a representative of the organization from committing the offence.[75]

SUMMARY

The following chart summarizes the above analysis, focusing specifically on the likelihood of establishing corporate criminal liability under s. 45 of the *Competition Act*, assuming participation by a senior officer and no evidentiary concerns. As demonstrated by this chart, the likelihood of establishing corporate criminal liability generally corresponds to the level of human control over the actions of the algorithm.

It is valuable to consider this analysis of liability against the positions submitted by the participants of the OECD Roundtable on algorithms and collusion. The U.S. paper notes that if competitors directly communicate to use an algorithm as a tool for price-fixing — as in the messenger situation or as in a hub-and-spoke scenario, the competitors would likely be liable for price-fixing.[76] However, the U.S. paper is clear that "absent concerted action" between competitors, there is no liability for price-fixing.[77] The U.S. paper does not address the possibility for algorithms alone to be considered to be communicating with one another.

The E.U. paper, while agreeing on the notion that explicit agreements between competitors to use algorithms to price-fix will likely violate price-fixing laws,[78] takes a more expansive view of potential liability in situations where algorithms interact without intentional human coordination. Of particular note, the E.U. paper considers the possibility of "taking an expanded interpretation of the notion of 'communication'"[79] under E.U. price-fixing laws, such that "one could argue that through repeated interactions, two firms' pricing algorithms could come to "decode" each other, thus allowing each one to better anticipate the other's reactions."[80] The E.U. paper further suggests that "one cannot fully rule out the possibility that more creative and novel types of interactions could in certain situations meet the definition of 'communication,'"[81] and that "[i]f this is or were to become possible in the future, the firms using such algorithms would remain liable for their behaviour. It is up to the firms using algorithms to ensure that their algorithms do not engage in illegal behaviour."[82]

---

[75] Archibald, Jull & Roach, *supra* note 65 at 5-28.11.

[76] US OECD Paper, *supra* note 19 at paras 16-17.

[77] *Ibid* at para 18.

[78] EU OECD Paper, *supra* note 19 at para 26.

[79] *Ibid* at para 33.

[80] *Ibid.*

[81] *Ibid.*

[82] *Ibid* at para 28.

Scenario	Establish *actus reus*?	Establish *mens rea*?	Defence?
Messenger	Likely	Likely	Potentially
Predictable agent	Unlikely, but possible via attribution rule	Likely	Potentially
Autonomous machine	Unlikely, but possible via attribution rule	Unlikely	Potentially
Hub-and-spoke	Likely	Likely	Potentially

Figure 2: Summary of Analysis

JUSTIFYING CRIMINAL LIABILITY FOR ALGORITHMIC PRICE-FIXING

This paper has focused on the question of whether it would be possible to legally establish corporate criminal liability for algorithmic price-fixing in Canada. However, what has not been discussed up to this point is whether we *should* establish such liability.

As demonstrated above, it appears that it would be difficult to establish corporate criminal liability for algorithmic price-fixing unless an explicit agreement between humans led to the price-fixing. Given this conclusion, the question then becomes whether we believe this is how our criminal law should operate.

This is a substantial and complex question, and this paper does not intend to provide a definite answer. However, the following analysis sketches the general contours of the philosophical debate that could occur around this point.

It is well-established that criminal law is intended to condemn and punish for wrongdoing.[83] The value in criminally punishing humans or corporations for algorithmic price-fixing may vary in line with different theories of criminal punishment.

A utilitarian account of criminal punishment provides the theoretical bedrock for criminal law in Canada, and focuses on the societal value of using the criminal justice system to deter particular conduct and rehabilitate those who commit undesirable conduct.[84] Utilitarianism seems to provide a strong justification for imposing criminal punishment in situations where humans

---

[83] Henry M. Hart Jr., "The Aims of the Criminal Law" (1958) 23:3 Law & Contemp Probs 401 at 405; *R. v. M. (C.A.),* 1996 CarswellBC 1000F, 1996 CarswellBC 1000, [1996] 1 S.C.R. 500, [1996] S.C.J. No. 28 (S.C.C.) at para. 82.

[84] See Stanley A. Cohen, "An Introduction to the Theory, Justifications and Modern Manifestations of Criminal Punishment" (1981) 27 McGill LJ; *R v M. (C.A.), supra* at paras 78-79, at which Lamer CJ highlights the viewpoint that a retributivist theory of

simply use pricing algorithms as a tool to carry out a price-fixing agreement. From a utilitarian perspective, a situation of this nature does not differ from any other price-fixing agreement.

However, the utilitarian value somewhat decreases in line with the level of human involvement or direction in the outcome generated by the algorithm. If an algorithm generates outcomes that were not specifically intended or directed by a human, it seems difficult to justify the use of criminal punishment to deter the occurrence of future outcomes that are similarly generated. The value of any such punishment would be broad and cumbersome; the principal effect would be to deter the use of any pricing algorithm that has the ability to learn and develop without human intervention. It is difficult to see how, in situations where price-fixing is an unintended act of algorithmic pricing, criminal punishment could act as a deterrent to the specific criminal outcome of algorithmic price-fixing without deterring the use of pricing algorithms writ large. There may be deterrent value in terms of encouraging humans to closely monitor the outcomes generated by their pricing algorithms, though in general, the use of criminal punishment in relation to algorithmic price-fixing is most soundly justified by utilitarian principles in situations where humans have agreed to a price-fixing arrangement.

Utilitarian theories of criminal punishment operate alongside normative theories, such as the retributive theory. A retributive account of punishment, a theory which also runs strong through Canadian criminal jurisprudence,[85] holds that criminal punishment should be used to "sanction the moral culpability of the offender."[86] Chief Justice Lamer, writing on behalf of a unanimous Supreme Court of Canada (S.C.C.) in *R. v. M. (C.A.)*, described retributive justice, and specifically differentiated retributive justice from vengeance:

> Vengeance, as I understand it, represents an uncalibrated act of harm upon another, frequently motivated by emotion and anger, as a reprisal for harm inflicted upon oneself by that person. Retribution in a criminal context, by contrast, represents an objective, reasoned and measured determination of an appropriate punishment which properly reflects the *moral culpability* of the offender, having regard to the intentional risk-taking of the offender, the consequential harm caused by the offender, and the normative character of the offender's conduct. Furthermore, unlike vengeance, retribution incorporates a principle of restraint; retribution requires the imposition of a just and appropriate punishment, and *nothing more*. As R. Cross has noted in *The English Sentencing System* (2nd ed. 1975), at p. 121: "The retributivist insists that the punishment must not be disproportionate to the offender's deserts."[87]

---

punishment can only justify criminal punishment if accompanied by utilitarian considerations.

[85] *R. v. M. (C.A.), supra* note 83 at paras 78-82; Morris J. Fish, "An Eye for an Eye: Proportionality as a Moral Principle of Punishment" (2008) 28:1 Oxford J Leg Stud 57.

[86] *R. v. M. (C.A.), supra* note 83 at para 79.

Another normative justification for criminal punishment can be gleaned from the expressive theory of punishment.[88] This view of punishment uses the imposition of criminal sanction to "communicate society's condemnation of that particular offender's conduct."[89] It has been described by the Supreme Court of Canada in regard to the purposes of criminal sentencing, as follows:

> [A] sentence with a denunciatory element represents a symbolic, collective statement that the offender's conduct should be punished for encroaching on our society's basic code of values as enshrined within our substantive criminal law. As Lord Justice Lawton stated in *R. v. Sargeant* (1974), 60 Cr. App. R. 74, at p. 77: "society, through the courts, must show its abhorrence of particular types of crime, and the only way in which the courts can show this is by the sentences they pass."[90]

Once again, it appears straightforward to justify criminal punishment under these normative principles in situations where humans have agreed to a price-fixing agreement using algorithms as the tool to carry out the agreement.

However, the question of whether normative principles can justify criminal punishment for outcomes generated by pricing algorithms without specific human direction is more complex. Normative justification is based on sanctioning "moral culpability" or expressing "society's condemnation" of a particular act or omission. However, unlike other criminal offences, our society does not have a clear moral position regarding the blameworthiness of a legal person for the unintended outcomes produced by semi-autonomous or autonomous machines that the legal person created. This question has broader ramifications beyond those associated with algorithmic price-fixing. Our societal norms regarding the human culpability of autonomously acting machines have yet to take form, and, until they do, it will be difficult to ground any criminal punishment for unintended algorithmic price-fixing in normative principles.

It is crucial to emphasize that utilitarian and normative justifications for criminal punishment are not mutually exclusive alternatives, but rather "operate in conjunction with one another to provide a coherent justification for criminal punishment."[91] Based on the discussion above, it is clear that both utilitarian and normative principles can justify criminal punishment for price-fixing agreements in which algorithms are used as the tool to carry out the agreement. The grounds for justifying punishment in situations with less explicit human intention to form a price-fixing agreement are significantly less solid.

---

87 *Ibid* at para 80 (emphasis in original).

88 See Joel Feinberg, "The Expressive Function of Punishment" (1965) 49:3 The Monist 397.

89 *R. v. M. (C.A.), supra* note 83 at para 81.

90 *Ibid.*

91 *Ibid* at para 82.

CONCLUSION

The principal issue considered in this paper, namely the intersection between algorithmic pricing and competition law, constitutes only one part of what is a much larger question. Artificial intelligence and semi-autonomous machine decision-makers have entered our economy and society with remarkable pace and ubiquity. Legal systems around the world have been slow to answer the questions posed by these technological developments.

A 2018 report of Canada's Competition Bureau on big data and innovation attempted to address some of these issues, and specifically discussed the impact of computerized algorithms on the enforcement of Canada's price-fixing laws.[92] The Bureau's report is clear on two issues. First, it affirms that the Bureau intends to work within the parameters of Canada's existing competition laws in order to address the issues lying at the intersection of price-fixing and computerized algorithms.[93] Second, the report is clear that formal agreements between competitors to fix prices using sophisticated algorithms will be viewed in the same vein as agreements to fix prices using less sophisticated means.[94]

The report also acknowledges the possibility that situations will arise where "cartel agreements are reached purely through interactions between different AI technologies, absent any direct human involvement."[95] However, the Bureau avoids issuing any guidance on this possibility, writing, "[t]he Bureau has observed no evidence of this type of collusion but is aware of the theoretical debate about how it might manifest. Nevertheless, without the benefit of evidence about the nature, or even feasibility, of such collusion, it is premature to provide guidance."[96]

This paper explored how a spectrum of possible situations involving human control over algorithmic price-fixing squares with Canada's current criminal law regarding collusion. Based on the analysis, it is difficult to challenge the legal or theoretical legitimacy of imposing criminal liability on humans and corporations for intentionally using algorithms to carry out price-fixing agreements. However, both the legal and theoretical legitimacy for imposing criminal liability are significantly undermined if pricing algorithms develop a price-fixing arrangement absent any human direction.

As such, a tension arises between the problematic nature of imposing criminal liability for outcomes generated without human direction, and the benefits associated with attempting to mitigate the occurrence of such anti-competitive outcomes. A provision for issuing a civil regulatory sanction, such as ss. 90 or 79 of the *Act*, presents a tool to resolve this tension. The use of a civil

---

92 Canada, Competition Bureau, *Big Data and Innovation: Key Themes for Competition Policy in Canada* (Gatineau: Competition Bureau, 2018).

93 *Ibid* at 9.

94 *Ibid* at 10.

95 *Ibid.*

96 *Ibid.*

provision would allow the Bureau to regulate anti-competitive outcomes generated by pricing algorithms while avoiding the difficulties associated with formally establishing the elements of the s. 45 criminal offence. Other than a situation in which humans use algorithms to carry out a formal price-fixing agreement, the complexity associated with algorithmic price-fixing merits a flexible regulatory approach that is not bound by the strict confines of criminal punishment.