"MOVE FAST AND BREAK THINGS": LAW, TECHNOLOGY, AND THE PROBLEM OF SPEED

Since computers entered into the mainstream in the 1960s, the efficiency with which data could be processed has raised regulatory questions. This is well understood with respect to privacy. Data that was notionally public – divorce proceedings, say – had long been protected through the "practical obscurity" of paper records. When such material was available in a single hard copy in a government office, the chances of one's acquaintances or employer finding it was remote. Yet when it was computerised and made searchable through what ultimately became the Internet, such practical obscurity disappeared. Today, high-speed computing poses comparable challenges to existing regulatory models in areas from securities regulation to competition law, merely by enabling lawful activities – trading in stocks, or comparing and adjusting prices, say – to be undertaken more quickly than previously conceived possible. Many of these questions are practical rather than conceptual. Nevertheless, current approaches to slowing down such decision-making – through circuit-breakers to slow or stop trading, for example – are unlikely to address all of the problems raised by the speed of AI systems.

Simon **CHESTERMAN**[1]
BA/LLB (Hons) (Melbourne), DPhil (Oxford);
Dean and Provost's Chair Professor, Faculty of Law, National University of Singapore.

I. Introduction

1 The financial markets opened in New York on Thursday, 6 May 2010, much as they did on any other morning. A headline in the *Wall Street Journal* warned of possible economic chaos in Greece; the European Union ("EU") and the International Monetary Fund were

1 The author is deeply grateful to Damian Chalmers, Miriam Goldby, Hu Ying, Arif Jamal, Jeong Woo Kim, Koh Kheng Lian, Kenneth Khoo, Lau Kwan Ho, Emma Leong, Lin Lin, Daniel Seng, Sharon Seah, David Tan, Tan Zhong Xing, Umakanth Varottil and others for their comments on earlier versions of this text. Invaluable research assistance was provided by Violet Huang, Eugene Lau, Ong Kye Jing and Yap Jia Qing. Errors and omissions are due to the author alone.

cobbling together a rescue package. On Wall Street itself, concerns about European debt had seen the Dow Jones Industrial Average, an index of market value, fall nearly 60 points to close the previous day at 10,868.[2]

2 As the bell rang at the New York Stock Exchange, stocks were expected to continue their decline. Uncertainty about a looming election in Britain and an upcoming jobs report further dampened sentiment. In Washington DC, the Senate was debating a bill on financial regulation – part of ongoing efforts to guard against a crisis like that sparked by subprime mortgages three years earlier. Trading commenced and, as predicted, the Dow maintained its downward trajectory. Some traders moved funds into gold, long seen as a safe haven in times of economic downturn. None of this was especially unusual: markets go down as well as up.

3 One thing that did go up was known by the acronym "VIX". Calculated by the Chicago Board Options Exchange, the volatility index is a measure of the variance of options from underlying share prices – essentially, the extent to which traders are betting that prices will change over time. A higher number theoretically means that the market could rise or fall, though VIX is also referred to as the "fear index". That Thursday morning, it had risen by more than 20%. Traders reassured themselves that this was still far below the heights reached during the global financial crisis of 2007–2008.

4 At 2.32pm, however, the market began to collapse. Within a quarter of an hour, the Dow lost nearly 1,000 points or almost a tenth of its value – the biggest point drop over the course of a single day in its history.[3] Shares in Proctor & Gamble, a blue-chip stock long seen as one of the market's most stable, fell by more than a third.[4] Consulting company Accenture essentially lost all of its value, the price of its shares plummeting from US$40 to US$0.01. For reasons that no one could explain, more than a trillion dollars in market value vanished in minutes. On the floor of the New York Stock Exchange, traders shouted or watched open-mouthed as their screens flashed with sell orders and phones rang off the hook. National Economic Council Director Lawrence Summers was pulled out of a meeting. At the White House, Treasury Secretary Tim Geithner hastily briefed President Obama about what some were already calling "Black Thursday".

---

2 Sebastian Moffett & Alkman Granitsas, "Europe Crisis Deepens as Chaos Grips Greece" *The Wall Street Journal* (6 May 2010).

3 Larger percentage drops occurred on Black Monday in 1987 and during the crash of 1929.

4 Tom Lauricella, "Market Plunge Baffles Wall Street" *The Wall Street Journal* (7 May 2010).

5 And then, just as quickly, the market recovered.

6 In 90 seconds, half the losses were reversed. By 3.00pm, the price of most stocks had returned to previous levels. In the dry prose of a report by staff of the key regulatory bodies, "trading resumed in a more orderly fashion".[5] The day ended with the Dow 347 points below its previous close – a 3.2% drop, but suggestive of a correction rather than a catastrophe.

7 Over subsequent weeks, analysts and regulators struggled to explain what had happened during that 30-minute period. Speculation was rife that a trader had accidentally triggered a massive sale of Proctor & Gamble stock, in what came to be known as the "fat finger theory". But attention soon turned to trading algorithms. After a five-month investigation, a government report concluded that a mutual fund's attempt to sell a large number of futures contracts had triggered the "Flash Crash". High-frequency traders ("HFTs") executing the sale – algorithms able to buy and sell stocks and options in a fraction of a second – were unable to find traditional purchasers and instead sold and resold the options to other HFTs. This generated what the report termed a "hot-potato" effect, as the same positions were rapidly passed back and forth between computer programs. In a 14-second period, more than 27,000 such contracts were concluded, accounting for almost half the total trading volume.[6]

8 The increased speed of information technology is an essential component of the artificial intelligence ("AI") systems that are at the vanguard of what has been called a fourth industrial revolution. Moore's law famously predicts that processing speed will continue to increase –

---

5 *Findings Regarding the Events of May 6, 2010* (Washington, DC: US Commodity Futures Trading Commission and US Securities and Exchange Commission, 30 September 2010) <http://www.sec.gov/news/studies/2010/marketevents-report.pdf> (accessed 1 December 2020) at p 9. See also Graham Bowley, "US Markets Plunge, Then Stage a Rebound" *The New York Times* (6 May 2010); Tom Lauricella & Peter A McKay, "Dow Takes 1,010.14-Point Trip – Biggest Point Fall, Before a Snapback; Glitch to Blame?" *The Wall Street Journal* (7 May 2010); Kara Scannell, "Market Tumult: Regulators Are Stumped by Drop" *The Wall Street Journal* (8 May 2010); Tom Lauricella, Scott Patterson & Carolyn Cui, "Computer Trading Is Eyed – Debate Turns to Absence of Circuit Breakers, Market Makers as Plunge Is Probed" *The Wall Street Journal* (8 May 2010); and Mary L Schapiro, "Examining the Causes and Lessons of the May 6th Market Plunge" (Washington, DC: US Securities and Exchange Commission, 20 May 2010) <http://www.sec.gov/news/testimony/2010/ts052010mls.htm> (accessed 1 December 2020).

6 *Findings Regarding the Events of May 6, 2010* (Washington, DC: US Commodity Futures Trading Commission and US Securities and Exchange Commission, 30 September 2010) at p 3 <http://www.sec.gov/news/studies/2010/marketevents-report.pdf> (accessed 1 December 2020).

doubling approximately every two years, as it has for half a century.[7] Though there are signs that the rate of increase is slowing, ever more efficient machines mean that the marginal costs of data storage and computing power are trending towards zero.[8] The increasing complexity of those systems means that, although general AI remains science fiction for the time being, current applications of narrow AI have already moved significantly beyond human cognitive abilities. As the 2010 Flash Crash demonstrated, there is also a danger that such systems can move faster than humans can control.

9 This article considers the regulatory challenges posed by speed. Many of the transformations in the digital economy are more accurately linked to the speed and efficiency of data processing rather than true cognitive ability or "intelligence" as such. Speed has, nevertheless, raised legal problems when rules designed for 20th-century society are confronted with the changing practices of the 21st. The article examines three of them.

10 The first is also the best known: the effacement of distance by the speed with which data can flow around the world. The focus here is the combination of speed with increasingly sophisticated software, posing difficulties for would-be regulators in areas from protection of intellectual property to combating "fake news".

11 Secondly, the author returns to the "Flash Crash" of 2010 and the efforts to accommodate high-frequency trading. In theory, algorithms executing trades are subject to the same regulations as the human brokers that set them in motion. In practice, the possibility of disruption or manipulation due to the speed at which those algorithms operate has led bourses to explore ways of slowing them down. There is also a larger argument that computer-based trading has changed not only the culture but also the very nature of the market.

12 A third set of problems concerns competition law, also known as antitrust law. The digital economy offers consumers access to information previously unimaginable in any traditional marketplace. Yet that information and more is also available to retailers who are able to use pricing software to maximise profits. In the past, anti-competitive conduct required proof of a meeting of the minds to collude on prices or abuse market dominance. The speed with which prices can be adjusted

7 Robert F Service, "Chipmakers Look Past Moore's Law, and Silicon" (2018) 361(6400) *Science* 321.

8 Jeremy Rifkin, *The Zero Marginal Cost Society: The Internet of Things, the Collaborative Commons, and the Eclipse of Capitalism* (New York: St Martin's Press, 2014).

today means that tacit collusion may take place without any intent on the part of market actors – or even without any formal co-ordination between their computer programs.

13 Individually, these challenges point to practical obstacles to regulation of information technology in a globalised world. Together, particularly when combined with AI systems that are autonomous[9] and opaque,[10] they show the danger that those systems will operate in a manner that is uncontainable, unstoppable or undetectable.

II. The globalisation of information

14 One of the most basic challenges posed by speed, built into the structure of the Internet itself, is the globalisation of information. The ability to access data almost instantly from almost anywhere on the planet and project it globally presents obvious challenges to legal regimes premised on territorially-bounded states. Those challenges are not conceptual so much as practical, often requiring co-ordination across jurisdictions. Here, discussion will be limited to a few brief examples that should suffice to explain the problem.

15 Protection of intellectual property rights, for example, has always been challenged by the ability to make copies. The replacement of analogue technologies – the tape recorder, the photocopier – with digital ones radically transformed the economics of copying: the laborious task of making one copy gave way to the ability to share music and other content at effectively no cost and without regard to distance.[11] Lawsuits and legislative changes[12] led to most media platforms adopting copyright policies and takedown protocols,[13] while others were shut down

9 See Simon Chesterman, "Artificial Intelligence and the Problem of Autonomy" (2020) 1 Notre Dame J Emerging Tech 210.

10 See Simon Chesterman, "Through a Glass, Darkly: Artificial Intelligence and the Problem of Opacity" *American Journal of Comparative Law* (forthcoming).

11 Indeed, various social media platforms encourage this by "nudging" users to share material that they did not create. See Corinne H Y Tan, "Technological 'Nudges' and Copyright on Social Media Sites" (2015) 2015(1) Intell Prop Q 62; and David Tan, "Fair Use and Transformative Play in the Digital Age" in *Research Handbook on Intellectual Property in Media and Entertainment* (Megan Richardson & Sam Ricketson eds) (Cheltenham: Edward Elgar, 2017) p 102.

12 Notably the Digital Millennium Copyright Act 1998 (US).

13 In 2020, for example, Facebook removed more than 400,000 pieces of content per month for copyright violation: "Intellectual Property" (Facebook, 2020) <http://transparency.facebook.com/intellectual-property> (accessed 1 December 2020). See further Daniel Seng, "The State of the Discordant Union: An Empirical Analysis of DMCA Takedown Notices" (2014) 18 Va JL & Tech 369; and Jennifer Daskal, "*Google Inc. v Equustek Solutions Inc.*" (2018) 112 Am J Int'l L 727.

completely.[14] Producers and distributors developed technical means to limit copying, but a certain amount of piracy is often priced in as the cost of doing business.[15]

16 As with the unauthorised sharing of intellectual property, the Internet also facilitates the unwanted dissemination of prohibited material. The speed with which information can spread across the globe regularly frustrates efforts to contain it, while also challenging the legal rules intended to deter or punish tortious or criminal behaviour.[16] Indeed, attempts to ban material in one jurisdiction may merely serve to increase its prominence – while not curtailing its availability from other jurisdictions. Again, this is not new: when Peter Wright's scandalous memoir of his career in MI5 was banned in the UK in the 1980s, that legal action almost certainly increased worldwide sales even before the ban was finally lifted.[17] More recently, organisations such as WikiLeaks have built disaggregated distribution into their operating model.[18]

17 Another example of the difficulties posed by the speed of information flow is the modern phenomenon of "fake news".[19] The ability for malicious rumours to be spread online had long been identified as a problem with respect to bullying and distorting share prices, but it was the 2016 US election that led to concerns that it could be used for larger political purposes also.[20] As with sharing of protected or prohibited material, the speed with which fake news flows is not a

14 *AMG Records Inc v Napster Inc* 239 F3d 1004 (9th Cir, 2001). See also Joseph Menn, *All the Rave: The Rise and Fall of Shawn Fanning's Napster* (New York: Crown, 2003).

15 Luis Aguiar, Jörg Claussen & Christian Peukert, "Catch Me If You Can: Effectiveness and Consequences of Online Copyright Enforcement" (2018) 29(3) *Information Systems Research* 656; P Jean-Jacques Herings, Ronald Peeters & Michael S Yang, "Piracy on the Internet: Accommodate It or Fight It? A Dynamic Approach" (2018) 266(1) European J Operational Research 328. See also Jeremy A Cubert & Richard G A Bone, "The Law of Intellectual Property Created by Artificial Intelligence" in *Research Handbook on the Law of Artificial Intelligence* (Woodrow Barfield & Ugo Pagallo eds) (Cheltenham: Edward Elgar, 2018) at pp 414–416.

16 Lord Anthony Grabiner, "Sex, Scandal and Super-Injunctions – The Controversies Surrounding the Protection of Privacy" (2012) 45 Israel L Rev 537.

17 Laurence Zuckerman, "How Not to Silence a Spy: Banned in Britain, an Agent's Memoirs Become Big-Selling News" *Time* (17 August 1987). See Peter Wright, *Spycatcher: The Candid Autobiography of a Senior Intelligence Officer* (New York: Viking, 1987).

18 Stephen M E Marmura, *The WikiLeaks Paradigm: Paradoxes and Revelations* (Cham: Palgrave, 2018).

19 Brian McNair, *Fake News: Falsehood, Fabrication and Fantasy in Journalism* (London: Routledge, 2018). The dissemination of false information is, of course, as old as human society itself.

20 *Report on the Investigation into Russian Interference in the 2016 Presidential Election* (Washington, DC: Department of Justice, March 2019) at pp 14–29 <http://www.justice.gov/storage/report.pdf> (accessed 1 December 2020).

problem caused exclusively by AI. Novel developments that are linked to new technologies, however, include automatically-generated content and so-called "deepfakes" – false content, such as doctored images and videos, that can be difficult to distinguish from genuine material.[21] All of this exacerbates the problem.

18 Government efforts to address the phenomenon of fake news have tended to focus on trying to correct it or contain it. Statutes introduced in Germany,[22] France,[23] Malaysia[24] and Singapore[25] enable public authorities to require social media sites to add corrections to or take down certain material within a designated time frame. Other approaches have emphasised responsibility for content, such as users being required to register under their real name, limiting the ability to share information widely, and straightforward censorship. China has used all three methods on sites such as Sina Weibo and WeChat.[26]

19 Social media platforms themselves long abjured any responsibility for the content that they host. Revelations of the sale of personal data to Cambridge Analytica in the context of the 2016 US Presidential election led to a series of efforts by Facebook, Twitter and others to exercise greater control over the dissemination of fake news. This included deleting accounts that violate community standards, prioritising posts by friends and family over those by publishers and businesses, and employing fact-checkers to add context to newsfeed items.[27] In 2018, Twitter deleted tens of millions of accounts that were suspected of being fake.[28] Violence

21 Zack Whittaker, "US Lawmakers Warn Spy Chief that 'Deep Fakes' Are a National Security Threat" *TechCrunch* (13 September 2018).

22 Netzdurchsetzunggesetz (NetzDG) 2017 (Germany) (Network Enforcement Act).

23 Loi organique no 2018-1201 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information 2018 (France); Loi no 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information 2018 (France). The French legislation was limited to during election campaigns.

24 Anti-Fake News Act 2018 (No 803 of 2018) (M'sia).

25 Protection from Online Falsehoods and Manipulation Act 2019 (Act 18 of 2019).

26 Ronggui Huang & Xiaoyi Sun, "Weibo Network, Information Diffusion and Implications for Collective Action in China" (2014) 17(1) Information, Communication & Society 86; Huiquan Zhou & Quanxiao Pan, "Information, Community, and Action on Sina-Weibo: How Chinese Philanthropic NGOs Use Social Media Authors" (2016) 27 Voluntas: Int'l J of Voluntary and Nonprofit Org 2433; James Griffiths, *The Great Firewall of China: How to Build and Control an Alternative Version of the Internet* (London: Zed Books, 2019).

27 Jonah Engel Bromwich & Matthew Haag, "Facebook Is Changing: What Does That Mean for Your News Feed?" *The New York Times* (12 January 2018); Kevin Kwang, "Facebook Expands Fact-Checking Initiative to Singapore Amid Challenges in Other Markets" *Channel NewsAsia* (2 May 2019).

28 Anthony Cuthbertson, "Twitter to Delete 6% of All Accounts in Huge Cull" *Independent* (London) (12 July 2018).

in India linked to misinformation spread through WhatsApp saw the messaging application in 2019 impose limits on the number of accounts to which messages can be forwarded.[29] The stakes were even higher in 2020 as concerted efforts spread falsehoods about the COVID-19 pandemic and the US presidential election.

20 Not even the most optimistic regulator believes that fake news will disappear anytime soon. Innovations such as deepfakes[30] and authentic-looking bot accounts point to the role that AI systems will play in both exacerbating the problem of fake news and offering means of addressing it.[31] Yet the underlying problem seems to be a human one. As a Massachusetts Institute of Technology study of a decade of Twitter postings showed, fake news is more novel and inspires more intense emotions than its truthful counterpart, with the result that lies spread more quickly than truth – and it is because humans are doing the sharing rather than robots.[32]

21 The globalisation of information has put more knowledge in the hands of more people than at any time in human history; in many repressive regimes, the Internet has played a liberating role precisely because of the difficulty of containing information. The structures that facilitate this are also barriers, however, to containing material that is proprietary, defamatory, or otherwise harmful. As AI systems play a greater role in generating content, efforts at containment – through data localisation, filtering, or otherwise slowing the flow of information – will run the risk of undermining the foundations of the digital economy and are at best likely to be a short-term fix for a fast-moving problem.

III. High-frequency trading

22 Speed has generated different practical problems in the world of high-frequency trading, in which algorithms buy and sell stocks or derivatives with an eye to making incremental profits on a large number of transactions. An indication of the premium put on speed is that a Chicago-based company spent US$300m laying a dedicated fibre-optic

29 Alex Hern & Michael Safi, "WhatsApp Puts Limit on Message Forwarding to Fight Fake News" *The Guardian* (21 January 2019).

30 Discussed at para 17 above.

31 Georgios Gravanis *et al*, "Behind the Cues: A Benchmarking Study for Fake News Detection" (2019) 128 Expert Systems with Applications 201; Hoon Ko *et al*, "Human-Machine Interaction: A Case Study on Fake News Detection Using a Backtracking Based on a Cognitive System" (2019) 55 *Cognitive Systems Research* 77.

32 Soroush Vosoughi, Deb Roy & Sinan Aral, "The Spread of True and False News Online" (2018) 359(6380) *Science* 1146.

cable to New Jersey in order to shave three milliseconds off the time it took data to travel from its offices to the stock exchange.[33] Today, HFTs are estimated to account for around half of all trades by volume in US and European markets.[34] Though profits in the US appear to have peaked,[35] Asian markets are seen as having significant capacity for growth in HFTs.[36]

23 The argument in favour of HFTs is that they provide liquidity to the market by increasing the number of buyers and sellers at any given moment, as well as helping in price discovery.[37] The danger is that because the programs operate so quickly, they can also increase price volatility and destabilise the market. In the 2010 Flash Crash, for example, US regulators concluded at the time that HFTs might not have been the cause of the crash, but at the very least they exacerbated its consequences.[38] The response was an expansion of trading curbs or "circuit breakers". These had been introduced in the wake of the 1987 Black Monday crash to prevent runs on the stock exchange caused by human panic. They operate as follows: if the market drops by a certain percentage,[39] trading can be paused for a period of time or for the rest of the day. The hope is that

33 Michael Lewis, *Flash Boys: A Wall Street Revolt* (New York: WW Norton, 2014) at pp 7–22; Megan Woodward, "The Need for Speed: Regulatory Approaches to High Frequency Trading in the United States and the European Union" (2011) 50 Vand J Transnat'l L 1359.

34 See generally Irene Aldridge & Steven Krawciw, *Real-Time Risk: What Investors Should Know About FinTech, High-Frequency Trading, and Flash Crashes* (Hoboken: Wiley, 2017).

35 Alexander Osipovich, "High-Frequency Traders Fall on Hard Times" *The Wall Street Journal* (21 March 2017); Gregory Meyer, Nicole Bullock & Joe Rennison, "How High-Frequency Trading Hit a Speed Bump" *Financial Times* (1 January 2018).

36 Hao Zhou & Petko S Kalev, "Algorithmic and High Frequency Trading in Asia-Pacific, Now and the Future" (2019) 53 Pac-Basin Fin J 186.

37 Jonathan Brogaarda *et al*, "High Frequency Trading and Extreme Price Movements" (2018) 128 J Fin Econ 253 at 254. *Cf* James Upson & Robert A Van Ness, "Multiple Markets, Algorithmic Trading, and Market Liquidity" (2017) 32 J Fin Markets 49; Donald MacKenzie, "'Making', 'Taking', and the Material Political Economy of Algorithmic Trading" (2018) 47 Economy and Society 501; and Brian M Weller, "Does Algorithmic Trading Reduce Information Acquisition?" (2018) 31 Rev Fin Stud 2184.

38 *Findings Regarding the Events of May 6, 2010* (Washington, DC: US Commodity Futures Trading Commission and US Securities and Exchange Commission, 30 September 2010) at pp 45–48 <http://www.sec.gov/news/studies/2010/marketevents-report.pdf> (accessed 1 December 2020). *Cf* Andrei Kirilenko *et al*, "The Flash Crash: High-Frequency Trading in an Electronic Market" (2017) 72 J Fin 967.

39 Until 1997, the thresholds were set by reference to a drop in points.

such a pause gives investors "more time to obtain information and make rational decisions".[40]

24 Under the New York Stock Exchange rules in force in 2010, these provisions would have kicked in to halt trading for half an hour if the Dow had dropped by 10% against a quarterly benchmark before 2.30pm, or the market would have been closed completely if it had fallen by 20% or more after 2.00pm. In the wake of the Flash Crash, these limits were revised to cover specific stocks that rise or fall more than 10% in value within a five-minute period.[41] The following year, the exchange-wide thresholds were tightened to suspend trading after a 7% drop of Standard & Poor's 500, a measure that includes 500 large publicly traded US stocks, against a daily benchmark rather than a benchmark set every three months.[42]

25 Other countries have followed suit.[43] In the EU, the Markets in Financial Instruments Directive II ("MiFID II") now imposes limits on high-frequency trading (and algorithmic trading more generally), adding metaphorical "speed bumps" to prevent disorderly trading and reduce market volatility.[44] Authorised traders must also disclose, among other things, how their algorithms work and who controls them. Trading data must be kept, with provision for modelling it as well as flagging unusual

40 Yong H Kim & J Jimmy Yang, "What Makes Circuit Breakers Attractive to Financial Markets? A Survey" (2004) 13 *Financial Markets, Institutions & Instruments* 109 at 121.

41 *Securities Exchange Act Release No 62252* (Washington, DC: Securities and Exchange Commission, 10 June 2010) <http://www.sec.gov/rules/sro/bats/2010/34-62252.pdf> (accessed 1 December 2020). See also E Wes Bethel *et al*, "Federal Market Information Technology in the Post Flash Crash Era: Roles for Supercomputing" (2012) 7(2) J Trading 9.

42 *Recommendations Regarding Regulatory Responses to the Market Events of May 6, 2010* (Washington, DC: Joint CFTC-SEC Advisory Committee, 18 February 2011) <http://www.cftc.gov/sites/default/files/idc/groups/public/@aboutcftc/documents/file/jacreport_021811.pdf> (accessed 1 December 2020); Notice of Proposed Rule Change Related to Trading Halts Due to Extraordinary Market Volatility (Washington, DC: Securities And Exchange Commission, Release No 34-65425; File No SR-ISE-2011-61, 28 September 2011).

43 Singapore introduced circuit breaker provisions in 2014 (Singapore Exchange Securities Trading Limited Rules, r 8.10A "Circuit Breakers and Cooling Off Periods") with Hong Kong doing so in 2016: Peter Wells, "Hong Kong Stock Exchange Introduces Circuit Breaker" *Financial Times* (22 August 2016); David R Meyer & George Guernsey, "Hong Kong and Singapore Exchanges Confront High Frequency Trading" (2017) 23(1) Asia Pac Bus Rev 63.

44 Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU 2014 (EU).

orders and establishing thresholds of price and volume beyond which a circuit breaker will kick in.[45]

26 The EU requirements highlight that market instability linked to HFTs is clearly not the same as human emotions causing a run on the market. The original circuit breakers offered time to make "rational" decisions. That is not generally a deficiency in HFTs.[46] Presumably in recognition of this, the New York Stock Exchange today stresses that even though it embraces "cutting edge, ultrafast technology, we believe nothing can take the place of human judgment and accountability."[47]

27 Any attempt to restrict the behaviour of HFTs confronts the question of whether and how they merit special treatment.[48] In principle, HFTs have access to the same information and trade on the same basis as other investors. Most regulatory efforts to date have focused on limiting market disruption and manipulation associated with their capacity to make many such trades in a short period of time. In practice, of course, speed also brings with it information asymmetry: the ability to process and trade on information before anyone else offers a clear advantage. Various HFTs therefore subscribe directly to news and market feeds in order to make trades almost immediately upon the release of notionally "public" data and assume a first-mover advantage.[49] Though not illegal, former New York Attorney-General Eric Schneiderman termed this "insider trading 2.0".[50]

28 Speed bumps and other means of slowing down HFTs could reduce that advantage.[51] Another approach is to restrict early access to

---

45 Tilen Čuk & Arnaud van Waeyenberge, "European Legal Framework for Algorithmic and High Frequency Trading (Mifid 2 and MAR): A Global Approach to Managing the Risks of the Modern Trading Paradigm" (2018) 9 Eur J Risk Reg 146.

46 Indeed, there is some evidence that the presence of algorithmic traders can make humans behave more rationally also: Mike Farjama & Oliver Kirchkampb, "Bubbles in Hybrid Markets: How Expectations about Algorithmic Trading Affect Human Trading" (2018) 146 J Econ Behavior & Org 248.

47 New York Stock Exchange, *Trading Information* (2020) <http://www.nyse.com/markets/nyse/trading-info> (accessed 1 December 2020).

48 Steven R McNamara, "The Law and Ethics of High-Frequency Trading" (2016) 17 Minn J L Sci & Tech 71.

49 This is particularly true if the system can anticipate other large orders and front-run them. Florian Gamper, "Is High Frequency Trading Fair? The Case of Order Anticipation" (Singapore: NUS Centre for Banking & Finance Law, 2016).

50 Abrams Rachel, "Attorney General Vows to Crack Down on 'Insider Trading 2.0'" *The New York Times* (9 January 2014); James J Angel & Douglas M McCabe, "Insider Trading 2.0? The Ethics of Information Sales" (2018) 147 J Bus Ethics 747.

51 Edwin Hu, "Intentional Access Delays, Market Quality, and Price Discovery: Evidence from IEX Becoming an Exchange" (Washington, DC: US Securities and Exchange Commission, Division of Economic and Risk Analysis Working Paper,

(cont'd on the next page)

market data.[52] More radical ideas include changing the way that exchanges think about time itself. One proposal is to replace the current system of orders, which treats time as continuous, with frequent batch auctions that treat time as made up of discrete units. Rather than executing trades in the order in which they are received, trades would be executed at discrete intervals – every tenth of a second, say. This would reduce the incentive to shave milliseconds off the placement of an order and the market distortions to which HFTs give rise.[53]

29 A second point of distinction concerns whether HFT users can and should be compelled to be more transparent about their algorithms than human traders are about their own investment strategies. This is now required by the EU regime, for example. The justification for special treatment is also typically tied to the possibility of disruption and manipulation of the market. Yet there is an argument that algorithmic and high-frequency trading have transformed not just how trades are made but how markets operate. In theory, brokers executing trades on the floor of an exchange are subject to the same basic rules of contract and securities regulation as those using mouse-clicks and algorithms. In practice, however, the move to computer-based trading has changed the culture of the market as well as the space of regulation.[54] In addition to the usual ups and downs of financial markets, this increases the risk of crises comparable to the 2010 Flash Crash. In 2012, for example, an error in a program used by the brokerage firm Knight Capital caused a loss of almost half a billion dollars and effectively spelled the end of the company.[55]

30 A more compelling explanation is that additional disclosure is necessary not merely to encourage stability and discourage manipulation but to make regulation possible in the first place. This is most evident in Germany, which went beyond the EU provisions in requiring that traders

7 February 2018) <http://www.sec.gov/files/07feb18_hu_iex_becoming_an_exchange.pdf> (accessed 1 December 2020).

52 Gaia Balp & Giovanni Strampelli, "Preserving Capital Markets Efficiency in the High-Frequency Trading Era" (2018) 2018(2) U Ill JL Tech & Pol'y 349 at 388–392.

53 Eric Budish, Peter Cramton & John Shim, "The High-Frequency Trading Arms Race: Frequent Batch Auctions as a Market Design Response" (2015) 130(4) Q J Econ 1547.

54 Marc Lenglet & Joeri Mol, "Squaring the Speed of Light? Regulating Market Access in Algorithmic Finance" (2016) 45 *Economy and Society* 201; Ann-Christina Lange, Marc Lenglet & Robert Seyfert, "Cultures of High-Frequency Trading: Mapping the Landscape of Algorithmic Developments in Contemporary Financial Markets" (2016) 45 *Economy and Society* 149.

55 Sandeep Yadav, "Operational Risk – A Case of Knight Capital" *Newstex Global Business* (13 July 2015).

flag orders generated by an algorithm so that they can be distinguished from human orders and that traders identify the algorithm in question.[56]

IV. Competition law

31 A special case of the accelerated flow of information linked to AI is the challenge that this poses for competition law. The rise of data analytics is making businesses more efficient and creating new opportunities for growth. Yet there is also clear potential for anti-competitive conduct.

32 For as long as capitalism has existed, the marketplace has been characterised by buyers and sellers watching prices and adjusting them in accordance with supply and demand. Those prices were once stamped on items on a shop floor; changing them was a decision that might take weeks to implement. Indeed, some items sold through coin-operated machines remained at the same price for decades. A bottle of Coca-Cola in the US, for example, cost the same – US$0.05 – between 1886 and 1959.[57]

33 Today, prices change in milliseconds. Dynamic pricing is the norm in retail, travel, sports and entertainment. Occasionally, the algorithms underpinning this produce curious outcomes – as when Peter Lawrence's book, *The Making of a Fly*, peaked at a sale price on Amazon of almost US$24m (plus US$3.99 shipping).[58] In general, however, digital marketplaces allow greater transparency and lower search costs, which should be good for competition. The ability to compare prices from different retailers should empower consumers to select cheaper options or demand premium services.[59] In reality, the picture is more complex.[60]

---

56 Hochfrequenzhandelsgesetz 2013 (Germany) (High Frequency Trading Act) amending, *inter alia*, the Börsengesetz (Stock Exchange Act) and the Wertpapierhandelsgesetz (Securities Trading Act) to require additional reporting on algorithmic trades. See also Nathan Coombs, "What Is an Algorithm? Financial Regulation in the Era of High-Frequency Trading" (2016) 45 *Economy and Society* 278 at 279. This finds some parallels in moves to require that "short" orders – whether executed by human or algorithm – be identified as such.

57 Daniel Levy & Andrew T Young, "'The Real Thing': Nominal Price Rigidity of the Nickel Coke, 1886–1959" (2004) 36 J Money, Credit, and Banking 765.

58 Ariel Ezrachi & Maurice E Stucke, "Artificial Intelligence & Collusion: When Computers Inhibit Competition" [2017] U Ill L Rev 1775 at 1781.

59 Nicolas Petit, "Antitrust and Artificial Intelligence: A Research Agenda" (2017) 8(6) J Eur Competition L & Prac 361.

60 See Ariel Ezrachi & Maurice E Stucke, *Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy* (Cambridge, MA: Harvard University Press, 2016) at pp 27–33.

34 Antitrust or competition law in various jurisdictions prohibits anti-competitive agreements and concerted practices.[61] A century ago, this might have meant gathering executives from competitor firms in a smoke-filled ballroom, as when Elbert Gary brought US steel manufacturers to a series of dinners at the Waldorf-Astoria a century ago, inviting them to tell each other "frankly and freely … what prices they were charging, how much wages they were paying their men, and … all information concerning their business".[62] Today, vastly more data is available. Sharing data is unlikely to be problematic if it is historical, or if it is shared with consumers and government agencies.[63] As data becomes available and can be analysed in real time, however, the question of whether a company itself is meaningfully deciding to disclose pricing information may become moot.

35 Similar problems arise in determining whether notional competitors are colluding. A collusive equilibrium is established if there is a common policy where adherence to the policy is monitored and deviations punished. As firms increasingly use price-monitoring algorithms to track competitors' actions, however, the algorithms themselves may trend towards such a "policy". If the price of an item is instantly matched by a competitor, for example, there is no incentive to reduce that price – indeed, the algorithms may conclude that raising prices in parallel is the rational response. Without evidence of direct or indirect communication between the parties, however, collusion may be difficult to establish.[64] If the algorithms themselves are proprietary, or exceptionally complex, it may be impossible.[65]

36 These are not merely theoretical concerns. In 2015, the US Department of Justice ("DOJ") charged the perpetrators of a price-fixing scheme that were selling posters through Amazon Marketplace. The scheme involved an algorithm that collected competitor pricing

61 See, *eg*, s 34 of the Competition Act (Cap 50B, 2006 Rev Ed).

62 William H Page, "The Gary Dinners and the Meaning of Concerted Action" (2009) 62 SMU L Rev 597.

63 See, *eg*, Wong Chun Han *et al*, "Data: Engine for Growth – Implications for Competition Law, Personal Data Protection and Intellectual Property Rights" (Singapore: Competition and Consumer Commission of Singapore, 16 August 2017) <https://www.cccs.gov.sg/resources/publications/occasional-research-papers/data-engine-for-growth> (accessed 1 December 2020).

64 Paolo Siciliani, "Tackling Algorithmic-Facilitated Tacit Collusion in a Proportionate Way" (2019) 10(1) J Eur Comp L & Prac 31 at 32.

65 Kay Firth-Butterfield, "Artificial Intelligence and the Law: More Questions than Answers?" (2017) 14(1) *Scitech Lawyer* 28.

information online and applied the sellers' pricing rules. According to the DOJ press release:[66]

> We will not tolerate anticompetitive conduct, whether it occurs in a smoke-filled room or over the Internet using complex pricing algorithms. American consumers have the right to a free and fair marketplace online, as well as in brick and mortar businesses.

37 This was, in fact, one of the simpler forms of anti-competitive conduct online. Behind it were human conspirators who had set the algorithm in motion precisely to undercut those outside the virtual cartel. More complex forms include situations when notional competitors adopt similar algorithms that, without formal co-ordination, set similar prices. Without human intent, does this amount to anti-competitive conduct? Still more difficult is the question of whether algorithms that process data concerning the entire marketplace will manipulate prices in a manner that is difficult or impossible to detect.[67]

38 Regulators are acutely aware of the difficulties. An Organisation for Economic Co-operation and Development background paper warned in 2016 that finding ways to prevent collusion between self-learning algorithms could be one of the biggest challenges competition law enforcers have ever faced.[68] "We're talking about a velocity of decision-making that isn't really human", a member of the US Federal Trade Commission observed. "All of the economic models are based on human incentives and what we think humans rationally will do. It's entirely possible that not all of that learning is necessarily applicable in some of these markets."[69]

39 Tacit collusion by algorithms raises the concern that one of the harms intended to be avoided by competition law – higher prices – will not be matched by a remedy.[70] As in the case of high-frequency trading, one suggestion has been to impose artificial delays in the form

66 Quoted in Ariel Ezrachi & Maurice E Stucke, "Artificial Intelligence & Collusion: When Computers Inhibit Competition" [2017] U Ill L Rev 1775.

67 Maurice E Stucke & Ariel Ezrachi, "Antitrust, Algorithmic Pricing, and Tacit Collusion" in *Research Handbook on the Law of Artificial Intelligence* (Woodrow Barfield & Ugo Pagallo eds) (Cheltenham: Edward Elgar, 2018) at pp 626–631.

68 "Big Data: Bringing Competition Policy to the Digital Era" (Paris: OECD, DAF/COMP(2016)14, 27 October 2016) at p 24 <http://one.oecd.org/document/DAF/COMP(2016)14/en/pdf> (accessed 1 December 2020).

69 David J Lynch, "Policing the Digital Cartels" *Financial Times* (9 January 2017).

70 Maurice E Stucke & Ariel Ezrachi, "Antitrust, Algorithmic Pricing, and Tacit Collusion" in *Research Handbook on the Law of Artificial Intelligence* (Woodrow Barfield & Ugo Pagallo eds) (Cheltenham: Edward Elgar, 2018) at p 636.

of a time-lag in price adjustment.[71] The alternative may be scrutinising prices to determine whether a given mark-up is too high, a laborious and potentially pointless exercise. As the European Commission conceded, with algorithms operating more independently, their decisions will increasingly conflict with a regulatory framework designed for "more predictable, more manageable and controllable technology".[72]

V. Conclusion: The problem with speed

40 "Move fast and break things" was an early motto at Facebook intended to push developers to take risks; the phrase appeared on office posters and featured in a letter from Mark Zuckerberg to investors when the company went public in 2012.[73] Over time, it came to be embraced as a mantra applicable to technological disruption more generally, adopted by countless Silicon Valley imitators. As Facebook matured, however, and as the potential harms caused by such disruption grew, the slogan fell from favour.[74]

41 The speed discussed here concerns processing power and connectivity rather than innovation, but it is likely that a similar reckoning will come for the digital economy, breathlessly referred to as

71 Paolo Siciliani, "Tackling Algorithmic-Facilitated Tacit Collusion in a Proportionate Way" (2019) 10(1) J Eur Comp L & Prac 31 at 34 (suggesting a latency of 12 hours in certain online marketplaces).

72 *Commission Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy* (Brussels: European Commission, SWD(2017) 2, 10 January 2017) at p 43 <http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A52017SC0002> (accessed 1 December 2020). A more optimistic view starts from the difficulty of policing tacit collusion between humans in the first place. In the absence of communication, it can be difficult to prove as well as hard to justify liability for what appears to be rational behaviour – taking a rival's prices into account when pricing one's own product. For algorithms, it would at least be theoretically possible simply to prohibit those that take interdependency of rivals into account. Many thanks to Kenneth Khoo for discussions on this topic. See, *eg*, Kenneth Khoo & Jerrold Soh, "The Inefficiency of Quasi-Per Se Rules: Regulating Information Exchange in EU and US Antitrust Law" (2020) 57 Am Bus LJ 45. On tacit collusion and facilitating practices generally, see Lawrence A Sullivan, Warren S Grimes & Christopher L Sagers, *The Law of Antitrust: An Integrated Handbook* (St Paul, MN: West, 3rd Ed, 2014) at pp 255–256.

73 Form S-1 Registration Statement of Facebook, Inc (Washington, DC: US Securities and Exchange Commission, 1 February 2012) <http://www.sec.gov/Archives/edgar/data/1326801/000119312512034517/d287954ds1.htm#toc287954_10> (accessed 1 December 2020).

74 Jonathan Taplin, *Move Fast and Break Things: How Facebook, Google, and Amazon Cornered Culture and Undermined Democracy* (New York: Little, Brown, 2017); Hemant Taneja, "The Era of 'Move Fast and Break Things' Is Over" *Harvard Business Review* (22 January 2019).

a fourth industrial revolution.[75] It has long been clear that such speed can pose challenges to regulation. This article examined three areas that exemplify those challenges as they relate to the exercise of public control over AI systems. The globalisation of information shows the difficulty of containing problematic activity in an interconnected world where speed has conquered distance. High-frequency trading points to the danger that the speed of decision-making can frustrate human attempts to stop it when things go off the rails. In competition law, tacit collusion by algorithms presents the real prospect that activity that would violate the law if perpetrated by humans may be impossible to detect if done by machines.

42 These problems – that the processing speed of AI systems may render some kinds of harm uncontainable, unstoppable or undetectable – apply to many of the other areas of activity challenged by new forms of technology. One way of addressing them is through slowing everything down: localising and compartmentalising data, introducing artificial latency in trading algorithms, and throwing sand in the gears of the digital marketplace.[76] Such an approach may be the only way of continuing to rely on regulatory tools designed for humans and operating on a human timescale, but runs the risk of undermining what makes those systems valuable in the first place.

43 It is also unsustainable. Whether or not one accepts predictions that processing power will continue to increase forever, the prospect of slowing it down or stopping any time soon is remote. New rules and new institutions will be required, together with at least some role for AI systems themselves in investigating and upholding the law.

44 For the time being, those tasks fall to human hands. In the wake of the 2010 Flash Crash, the regulators' report cited earlier was criticised for blaming a single large mutual fund for inadvertently triggering the market collapse.[77] In addition to the various safeguards put in place soon afterwards – circuit-breakers, speedbumps and so on – the investigation

75 See, *eg*, Klaus Schwab, *The Fourth Industrial Revolution* (New York: Crown, 2017).

76 The International Committee of the Red Cross, for example, has called for AI systems deployed in conflict zones to operate at "human speed" rather than "machine speed". See "Artificial Intelligence and Machine Learning in Armed Conflict: A Human-Centred Approach" (Geneva: International Committee of the Red Cross, 6 June 2019) at p 7 <http://www.icrc.org/en/document/artificial-intelligence-and-machine-learning-armed-conflict-human-centred-approach> (accessed 1 December 2020).

77 *Findings Regarding the Events of May 6, 2010* (Washington, DC: US Commodity Futures Trading Commission and US Securities and Exchange Commission, 30 September 2010) at p 14 <http://www.sec.gov/news/studies/2010/marketevents-report.pdf> (accessed 1 December 2020). The fund was later revealed to be Waddell & Reed.

into the cause of the crash continued. As it did, the focus moved from rogue algorithms to a single rogue trader.

45 The arc of the moral universe is long, as Martin Luther King Jr famously intoned, but it bends towards justice. It was almost five years later that a London-based dealer was arrested for his role in causing the crash. Criminal charges brought by the US Department of Justice accused Navinder Singh Sarao of using an automated trading program to manipulate the market by "spoofing" – offering US$200m worth of fake bets that drove prices down, modifying them 19,000 times, and then cancelling them before they could be completed.[78] As the market fell, he sold futures contracts only to buy them back at a lower price; when the market began to recover, he bought futures contracts and sold them at a higher price.[79] He was extradited to the US and pleaded guilty to market manipulation that had netted him some US$40m.[80]

46 The indictment quoted e-mails in which he had requested technical support for an off-the-shelf trading program, so that he would be able to enter "multiple orders at different prices using one click" and to add "a cancel if close function", so that an order would be cancelled before it could be completed.[81] Dubbed by British media "the Hound of Hounslow", some saw poetic justice in the fact that Sarao had later himself been conned out of virtually all of his ill-gotten gains.[82] As part of a plea deal, he went on to assist US regulators in prosecuting others for market abuse.[83]

---

78 Jennifer Rankin, "'Flash Crash' Trader Released on Bail" *The Guardian* (14 August 2015).

79 "Futures Trader Charged with Illegally Manipulating Stock Market, Contributing to the May 2010 Market 'Flash Crash'" (Washington, DC: Department of Justice, 21 April 2015) <http://www.justice.gov/opa/pr/futures-trader-charged-illegally-manipulating-stock-market-contributing-may-2010-market-flash> (accessed 1 December 2020).

80 Lindsay Whipp & Kara Scannell, "'Flash-Crash' Trader Navinder Sarao Pleads Guilty to Spoofing" *Financial Times* (10 November 2016).

81 *United States of America v Navinder Singh Sarao: Criminal Complaint* (Chicago: United States District Court, Northern District of Illinois, Eastern Division, 15 CR 75, 11 February 2015) at paras 15–16 <http://www.justice.gov/sites/default/files/opa/press-releases/attachments/2015/04/21/sarao_criminal_complaint.pdf> (accessed 1 December 2020).

82 "How the Flash Crash Trader's $50 Million Fortune Vanished" *Bloomberg* (10 February 2017).

83 Gregory Meyer & Philip Stafford, "Flash-Crash Trader Helps US in Fight against Market Abuse" *Financial Times* (30 January 2018). Sarao was later sentenced to one year of incarceration at his parents' home in Hounslow – returning to the very bedroom from which his crimes had been committed in the first place. Dominic Rushe & Simon Goodley, "'Flash Crash' Trader Sentenced to One Year Home Incarceration" *The Guardian* (28 January 2020).

47 Far from algorithms run amok, the software behind the 2010 Flash Crash faithfully executed the tasks Sarao had asked of it. Though suggestive of the kinds of harm that trading algorithms might cause, then, the crash itself could hardly be blamed on them. It did, however, show the potential for future harms when AI systems operate not only quickly, but also autonomously and opaquely. Containing, stopping or even detecting such systems will stretch or exceed existing regulatory tools, perhaps forcing a debate over whether it is more important to move fast, or to avoid things being broken.