



# Spoofing: Law, materiality and boundary work in futures trading

Donald MacKenzie

To cite this article: Donald MacKenzie (2022) Spoofing: Law, materiality and boundary work in futures trading, *Economy and Society*, 51:1, 1-22, DOI: [10.1080/03085147.2022.1987753](https://doi.org/10.1080/03085147.2022.1987753)

To link to this article: <https://doi.org/10.1080/03085147.2022.1987753>



© 2021 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group



Published online: 30 Nov 2021.



Submit your article to this journal [↗](#)



Article views: 611



View related articles [↗](#)



View Crossmark data [↗](#)



# Spoofing: Law, materiality and boundary work in futures trading

Donald MacKenzie 

## Abstract

Spoofing (canonically: ‘bidding or offering with the intent to cancel the bid or offer before execution’), once a valued skill in face-to-face trading, has become a crime punishable by jail. Echoing Riles’s call for greater attention to law in research on finance, this paper analyses the interwoven processes of this dramatic shift, including trading’s changing material form, contingencies such as the Congressional response to the global financial crisis, and, above all, the use of criminal (not just civil, administrative) law. Criminal law’s particularly strong boundary work – specifically the first criminal indictment and jail sentence for spoofing – rendered earlier ambivalent attitudes and inconsistent enforcement untenable. Nevertheless, drawing a boundary between spoofing and legitimate trading remains work-in-progress, with simultaneously legal, material and moral dimensions.

**Keywords:** spoofing; social studies of finance; law; trading pits; high-frequency trading; market surveillance.

Prohibited transactions ...

It shall be unlawful for any person to engage in any trading, practice, or conduct on or subject to the rules of a registered entity that ... is, is of the character of, or is commonly known to the trade as, “spoofing” (bidding or offering with the intent to cancel the bid or offer before execution) ... .

(US Commodity Exchange Act, section 4c, as amended by the 2010 Dodd–Frank Wall Street Reform and Consumer Protection Act, section 747)

*Donald MacKenzie, University of Edinburgh, United Kingdom. E-mail: D.MacKenzie@ed.ac.uk*

Copyright © 2021 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group. This is an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.



That market exchange is saturated with moral judgements – and pervasively so, not just when markets have an overt ethical dimension – is well understood in economic sociology, economic anthropology, social studies of finance and related fields (see, e.g. Fourcade & Healy, 2007). Much, however, remains to be learned: about how moral judgements change; how they are embedded in exchange's materiality; how they interweave with law. Those are this paper's themes.

It explores them via the topic of spoofing, canonically defined in the 14 words in brackets above. Spoofing is a rich topic for three reasons. First, this is indeed an area in which moral judgements have changed. As recently as 30 years ago, bidding to buy a financial instrument, or offering to sell it, while intentionally and successfully avoiding entering into a transaction, was a desirable, even a praiseworthy skill, employed to hide one's intentions in contexts such as the crowded face-to-face trading pits of Chicago's futures exchanges. It has now become a crime worthy of jail. Second, this shift is inextricably connected to trading's changing materiality, as face-to-face trading among humans has been replaced by electronic trading in which most actors are computer algorithms. Third, though, the shift is not a mere epiphenomenon of changes in trading's materiality, but a process that is both complex (intimately involving law) and to a degree local: manifest most dramatically in US futures trading, and centred above all in Chicago.

There is only a small social science literature on spoofing, with three main existing contributions. The first, Zaloom's superb participant-observation study of face-to-face trading in Chicago and electronic trading in London, does not focus on spoofing but contains what is now historically relevant information (Zaloom, 2006, pp. 157–158), drawn on below. The second, Arnoldi (2016), discusses an example of spoofing on a European exchange and an early administrative enforcement action by the US Securities and Exchange Commission (SEC). Although ultrafast high-frequency trading (HFT) algorithms are commonly portrayed by their critics as indulging in spoofing, Arnoldi rightly emphasizes HFT's vulnerability to spoofing. He suggests that the crackdown on spoofing results from the need to protect algorithms indispensable to today's trading.

In the third contribution, Pardo-Guerra (2019a, 2019b) argues that the order books (explained below) that form the infrastructure of electronic trading are a 'moral technology': they were, e.g. seen by their early proponents as permitting trading that would be 'fairer, more just, and more equal' (Pardo-Guerra, 2019a, p. 240) than among crowds of sweating bodies in trading pits. Spoofing, he suggests, violates 'a shared, moralized expectation of what order books ought to be' – 'depositories of "truthful" intentions' (Pardo-Guerra, 2019b, p. 117).

Arnoldi and Pardo-Guerra provide crucial insights. However, what they focus on (the vulnerability of HFT algorithms to spoofing; the implicitly moral nature of order books) are general factors that one would expect to

be evident – and empirically *are* evident, at least to some degree – across all markets in which HFT and order books are prevalent. Yet actual outcomes vary. There are, e.g. national differences: to my knowledge, spoofing has been criminally prosecuted only in the United States. Even US markets differ considerably: almost all prosecutions concern the market focused on here, futures.<sup>1</sup> To understand such differences, we have to consider not just ‘law in books’ (i.e. statute law), which can be read as outlawing spoofing in all US – and also all UK – financial markets, but also examine whether and how law in books is translated into what Pound (1910) famously called ‘law in action’.

In arguing that law, a peripheral concern in the existing literature on spoofing, has to take centre stage, this paper responds (belatedly, I confess) to Riles’s (2010) call for greater attention to law – with its explicit prohibitions and compulsions, its ‘must, shall, and will’ (p. 806) – in the social studies of finance and related fields. There have already been valuable responses, notably Milyaeva (2013) on legal culture, as well as a bigger literature on the regulation of, e.g. electronic markets: see Lenglet (2011), Lenglet and Mol (2016), Coombs (2016), and – particularly relevant here because of his detailed attention to surveillance – Williams (2009, 2012). The crackdown on spoofing is, however, distinctive in that it has involved *criminal* law to a greater extent than most regulation and surveillance.

The same ‘law in books’ can sometimes be applied in either a civil law action or a criminal law prosecution. Most of the enforcement of rules against spoofing has been civil: disciplinary action by an exchange or administrative action by a regulator (see the lists in Canellos *et al.*, 2016; Ray *et al.*, 2020). Exchanges typically suspend the perpetrator from trading for a limited period and impose a relatively modest monetary penalty. When a government regulator takes administrative action against spoofing, the suspension is often longer (perhaps around a year), and the civil monetary penalty typically larger. But it is not usually crushingly large, and most such administrative actions end in an agreed settlement, often with the alleged perpetrator neither admitting nor denying culpability. Criminal prosecution and the prospect of jail are entirely different matters, and that has given such prosecutions considerable significance, despite their much smaller number. The ‘must’ – and especially the ‘must not’ – of criminal law has a quite distinctive force.

Law should not, of course, be conceived of as a self-standing domain: it interweaves intimately with morality, the materiality of economic life, political economy and much else besides. That interweaving is complex and beyond the scope of a single paper. My focus here is simply on one theme: the material/moral/legal boundary work involved in defining, outlawing, detecting and punishing spoofing. ‘Boundary-work’ was given its name by Gieryn (1983) in an investigation of how scientists differentiate science from ‘pseudo-science’ (p. 781), and the term subsequently entered the argot of the social sciences at large: see, e.g. Lamont (2000). Within economic sociology, Zelizer’s (2012)

investigations of boundary work have been particularly influential (although she prefers the broader notion of ‘relational work’):

in all economic action ... people engage in the process of differentiating meaningful social relations. ... [P]eople erect a boundary, mark the boundary by means of names and practices ... designate certain sorts of economic transactions as appropriate ... bar other transactions as inappropriate ... .

(Zelizer, 2012, p. 145)

My phrase – ‘material/moral/legal boundary work’ – is ugly, and will mostly be abbreviated simply to ‘boundary work’, but the triple adjectives go to the heart of the paper’s argument. Distinguishing between legitimate and illegitimate forms of trading has inextricably interwoven material, moral and legal aspects, and no one aspect decisively trumps the others. Without the force of law, for example, a moral distinction may lack weight, but law without the material capacity to detect and provide evidence of a crime can remain mere ‘law in books’, not ‘law in action’, while even clearly framed law and assiduously gathered evidence may not guarantee a conviction if a jury cannot be convinced that the accused is in a strong sense morally implicated in a crime.

That the crackdown on spoofing involves material/moral/legal *work* points to a hidden trap in the notion of ‘boundary work’. It is too easy to think of a boundary, once collectively agreed upon (and, e.g. defined in statute law), as a Durkheimian ‘social fact’, to be treated as a ‘thing’, as simply there: detecting violations of the boundary may still involve work, but the boundary itself no longer does. But the ‘finitist’ sociology of science of Barnes and Bloor (along with ethnomethodology and the late Wittgenstein) suggests that, even in the sciences, conceptual boundaries do not unequivocally divide up in advance the space of all possible events, actions or entities (see, e.g. Barnes *et al.*, 1996). All that we have in practice is a finite set of agreed-upon instances of A, and another finite set of instances of not-A. When we come across a new particular instance, the decision whether to classify it as A or not-A is in principle an open-ended one.

Practitioners of law, especially in common law jurisdictions such as the United States, often seem implicitly finitist in how they understand their practices: what, for instance, does precedent consist in, if not a set of agreed-upon instances? Halpérin (2011) points out that there is an important current of ‘rule-skepticism’ in American legal theory, which denies the ‘determinacy of rules in empirical legal situations’, focusing instead on ‘judicial decisions or actions’ (p. 52). And indeterminacy is precisely what we find here. It is important that the Commodity Exchange Act now explicitly prohibits spoofing (‘law in books’ does matter), but, as we shall see, its words, quoted at the start of the paper, do not on their own suffice to bisect the activity of trading, so to speak: to divide it into actions that clearly constitute spoofing and those that unequivocally do not.

This introduction is followed by a brief section on data sources. The third section examines how traders in Chicago’s pits morally evaluated their peers’ conduct, in particular conduct that resembled what is now defined as illegal spoofing. The fourth section discusses the often-ambivalent attitudes taken to spoofing in electronic trading’s early days. The fifth section examines the crucial legal boundary work: the drafting of the Dodd-Frank amendment and the first criminal prosecutions for spoofing. The paper’s penultimate section emphasizes that this boundary work inevitably continues. The final section is the conclusion.

## Data sources

The research reported here is part of a broader study in which the author interviewed 337 financial-market participants, most of them in the four leading global centres of HFT: New York, Chicago, Amsterdam and London. Participants included, e.g. 86 practitioners of HFT, 47 traders of other kinds, and 33 brokers or dealers (see [Table 1](#)). Spoofing was only one topic covered by these interviews (for others, see MacKenzie, 2021). I did not, for example, expect any traders to tell me that they spoofed, and none did. I directly contacted two traders who had received substantial civil penalties for spoofing, but – again, not to my surprise – they did not agree to interviews. Several traders, though, indicated that they disagreed with at least some aspects of the crackdown on spoofing. None offered an all-out defence of it, but two of their partial defences are quoted below.

Although I did not know this when I approached them, five of my trader interviewees turned out to have initiated or been involved in regulatory action and/or criminal prosecution of alleged spoofers. To understand the crackdown on spoofing, though, I needed to do more than talk to traders. Particularly useful were interviews with four lawyers who have been directly involved in spoofing cases, and the topic also came up in interviews with surveillance specialists, regulators and exchange staff. (In what follows,

Table 1 Interviewees

High-frequency traders	86
Traders for investment-management firms	10
Practitioners of other forms of algorithmic trading	25
Manual traders	12
Dealers and brokers	33
Regulators, lawyers, etc	31
Exchange staff	87
Suppliers of technology	32
Market analysts	21
Total	337

interviewees are anonymized by two-letter codes: codes for traders have an initial T; lawyers L; regulators and surveillance specialists, R; exchange staff, E.)<sup>2</sup> I was given demonstrations of two anti-spoofing surveillance systems, took part in a training session on preventing spoofing, and was given access to the transcript of the first criminal trial for spoofing.

As already noted, the crackdown on spoofing has been particularly vigorous in US futures trading, which is centred on Chicago. (A ‘future’ is a standardized, exchange-traded contract roughly equivalent economically to one party undertaking to buy, and the other to sell, a set quantity of an underlying asset on a given future date, at a price agreed at the contract’s inception. Originally, Chicago’s markets traded futures on agricultural commodities, but from the mid-1970s onwards they expanded decisively into financial futures.) My fieldwork included 12 visits to Chicago (from October 2011 until shortly before the onset of the coronavirus epidemic), on which traders met on previous trips were often re-interviewed, enabling tracking of the crackdown in close to realtime. Research for MacKenzie (2006) had also taken me to Chicago in 1999–2000, when its famous open-outcry trading pits still flourished; that earlier research too is drawn on in the next section.

### **The moral order of the trading pit**

Watching constant jostling among the traders in Chicago’s crowded pits from visitor galleries (open until 11 September 2001), it was easy to imagine that pits were simply places of competition among self-interested, atomistic, amoral individuals. But a trader told me in November 2000, his words reflecting male dominance of pits:

This [Chicago] is a place where people think very simple in terms of people and markets. Black. White. Good. Bad. There’s an invisible sheet with an invisible line down the middle of it. This is a good guy. This is not a good guy. Nobody’s on that line. They’re either a good guy or a bad guy. Very long memories.

Hundreds of traders could crowd into a big pit, but they wore jackets prominently bearing their three or four-letter trading-floor IDs, and often stood in exactly the same spot every day. Much of their behaviour was therefore open to scrutiny by their fellow traders, even if the ‘invisible line’ was neither unequivocal nor fully consensual.

Bids and offers were shouted out – hence ‘open outcry’ – or hand-signalled using fingers to indicate prices and quantities. If several traders were bidding or offering at the same price, exchanges’ formal rules required traders to enter into a deal with the person first ‘heard’ or ‘seen’. But that was often ambiguous, and this could be used to punish or reward. Traders who had broken a pit’s informal rules too badly could find themselves permanently inaudible and invisible. Brokers (who brought to the pit orders from external clients such as banks,

big hedge funds, major corporations, etc.) often selectively heard or saw traders who previously had helped them execute a client's order in difficult circumstances, and that was widely regarded as legitimate; far more controversial were those brokers who preferred to hear or see traders who were affiliated to the same business group.

Deals agreed verbally or by hand signal and eye contact could not, in practice, be enforced legally, but a trader who made a deal and later denied doing so would find themselves frozen out. Nor was it acceptable for traders to refuse to enter into a deal if their raised hands were signalling a bid or offer, or they were shouting one out. As pit traders put it, a bid or offer remained valid while 'the breath is warm':

if you yelled 'six bid' and put two hands up in the air and someone said 'sold', if you back away from it, the whole pit would call you out and they wouldn't trade with you any more.

(Interviewee TA)

What, though, if a trader unequivocally signalled a bid or an offer, but then lowered their hands and allowed their breath to cool, and had intended to do that all along? By today's criteria that would be spoofing, says TA, but 'it sounds like a normal day in the pit. We spoofed all the time.' Traders were, for example, sometimes able to guess that a client was intending to buy on a large scale, perhaps because the broker known to act for that client was walking towards the pit. They might then, said interviewee TB, sometimes bid simply to drive the price up, rather than themselves actually wanting to buy at those temporarily inflated prices.

Issues of that kind meant that brokers often felt the need to hide their intentions. If, for example, they intended to buy, they might nevertheless also shout or hand signal offers to sell, while not actually intending a sale; interviewee LA reports that his brokerage's clients often 'expected' their brokers to do this. Such behaviour would now be classed as spoofing, but in the pits it was, LA says, 'considered to be good brokerage' – akin, as TC puts it, to bluffing in poker: 'not something that was thought of as wrong, immoral or illegal. In fact, it was in some ways admired, I think'.

I know of no attempt to curtail this 'bluffing' by the futures-market government regulator, the US Commodity Futures Trading Commission (CFTC). Law-enforcement focused on other matters, particularly on the handling of orders from external clients. The embodied materiality of pit trading was, however, a formidable obstacle to external scrutiny. Pits could be videotaped, but it was hard to spot subtleties of bodily behaviour: 'somebody winked', says LB, 'who knew whether they winked or if they didn't?' In the late 1980s, therefore, the FBI assigned four agents to work undercover in Chicago's pits, wearing hidden tape recorders (to my knowledge, the only full-blown investigation of this kind ever within a major financial institution).



Some of the resulting prosecutions led to convictions, but others failed in the face of material, legal and moral difficulties: poor quality audio-recordings (the entire trading floor was noisy, not just the pits themselves); trials that could last for months and hinged on technicalities that were difficult for a lay jury to grasp; at least one jury member who was uncertain whether the rule-breaking at issue qualified morally as criminal behaviour (Greising & Morse, 1991, pp. 282–287). Electronic trading, nascent in the 1980s, was therefore often welcomed as more readily susceptible to surveillance: it left a permanent record of every bid, offer and trade. An SEC Commissioner, for example, told a commodities law conference: ‘electronic order entry systems ... can help prevent many ... abuses’ (Grundfest, 1989, p. 8). But drawing a boundary between legitimate and illegitimate conduct in electronic trading was to turn out to be quite unexpectedly difficult.

### ‘A purity in market price’

The move of trading from pits to screens involved a shift from the voices and actions of familiar, recognizable human bodies to anonymous binary digits. A modern order book is an electronic file containing an anonymous list of the bids to buy the financial instrument being traded (and the offers to sell it) that have not yet been executed or cancelled: see [Figure 1](#). The balance between offers and bids summarizes the supply and demand for the instrument being traded, and is thus crucial information, both for human beings trading electronically using keyboard and mouse and for the computer algorithms that soon joined them.

Hence, the primary motivation for spoofing: bids or offers can be added to the order book, not in the hope that they will be executed, but because the resultant altered balance between bids and offers will influence other humans’ or algorithms’ actions. During a demonstration of a spoofing-detection system (using pre-recorded data), one trader’s accumulated trading

	BIDS TO BUY		OFFERS TO SELL
\$41.49	100    100    200		\$41.50
\$41.48	50    30		\$41.51
\$41.47	100		\$41.52
\$41.46	50    100    100    100		\$41.53
\$41.45	200		\$41.54

Figure 1 An order book

position was pointed out to me: ‘He’s long ... he’s unwinding a long position’, i.e. selling his holdings of the financial instrument in question. The trader, though, had also placed a large bid to buy. This created the impression of many more bids than offers, suggesting a coming price rise, and helping the trader make his intended sales at a favourable price. He cancelled the bid once its work was done. If he had intended all along to cancel it, his trading fell within the scope of the legal definition of spoofing quoted at the start of this paper.

Tactics of this kind seem to have become common almost as soon as electronic trading became widespread, both as a way of unwinding trading positions accumulated for other reasons (as in the above example), and as a direct money-making strategy. In the latter, a spoofer could, for example, first place a big spoof offer and so hope to buy at a temporarily low price, then reverse the strategy: place a spoof bid, causing prices to rise, and so be able to sell at a profit. Zaloom (2006, pp. 157–158) reports spoofing taking place in electronic futures trading in London as early as autumn and winter 2000, which confirms, e.g. my interviewee TD’s retrospective report of spoofing’s prevalence. It required little technical sophistication: a human being could (and still can) spoof using a keyboard and mouse, although the need to cancel the spoof bid or offer quickly (to avoid the risk of it being executed) has often led more recent spoofers to use computer programs to do the cancellation.

Vulnerability to spoofing, though, seemed greater among algorithms. In what interviewee TE calls ‘normal trading’ (i.e. without spoofing), machines’ data-processing capacities give them the advantage over humans, he says. ‘But somehow for spoofing, when you eyeball it, it’s always obvious for a human, but very difficult for the [algorithmic] model, somehow’: the requisite pattern-recognition task is hard to program. Zaloom’s fellow human traders seem almost to have relished the presence of spoofers (e.g. sometimes executing against spoof orders, intimidating the spoofer into liquidating the resultant unwanted trading position at a loss). However, just as Arnoldi (2016) suggests, spoofing was a deeper and more persistent problem for HFT firms, which were rapidly growing in scale from the early 2000s onwards.

The balance of bids and offers is a crucial input into HFT algorithms’ decision-making (MacKenzie, 2021). For example, a large excess of bids will often lead algorithms to buy, or themselves to place bids that reinforce the effects of the spoofer’s activity. If the spoofer then changes direction, and in particular starts not just placing offers but aggressively selling by executing against existing bids, an HFT algorithm can incur a substantial loss. This aggressive form of spoofing is known as ‘flipping’. A flipper is ‘going to entice us [our algorithms] to add’, in this instance to bid to buy, says high-frequency trader TF, ‘and then fill our order [execute against TF’s algorithm’s bid] in a market that’s moving in the opposite direction [i.e. as prices fall]’.

That happened to his firm’s algorithms time and time again, says TF: ‘it’s crushed us over the years’. His firm developed machine-learning systems to detect spoofing and flipping, tried to avoid order-book situations and

markets in which they were particularly prevalent, and reported them to the relevant exchange and regulatory body. Even as late as 2014, though, exchanges and regulators were often not fully equipped for the difficult material task of detecting spoofing in the dauntingly huge volumes of order-book data that a modern electronic exchange continuously spews out. That April, TF told me that his firm was ‘trying to help them [the regulator] out’ by supplying ‘visualization tools’ that would enable its staff to see in market data what TF and his colleagues believed were unequivocal traces of flipping. The firm’s efforts did eventually bear fruit in civil enforcement action by the regulator, but not before, interviewees report, tens of millions of dollars – or perhaps more – had been made from flipping.

Again as Arnoldi (2016) reports, my interviews suggest that, in the early days of automated trading, complaining about spoofing often had little effect. One former trader (EA) ‘complained to my complaints department and they just laughed at me and said “you should just fix your system”’. Another trader, TG, describes exchanges as ‘reluctant to make a fuss’ about spoofing, because, he says, they feared damage to their reputations. TH reported that his firm had complained about spoofing to the exchanges on which it traded, and received the response: ‘why is this wrong?’ TI, a former exchange official, had received such a complaint, and had promised to investigate it, but professed himself shocked that the HFT firm seemed unable to stop its algorithms being spoofed:

I kept telling them, ‘look, the inquiry has been launched, but this isn’t going to stop today, we can’t turn off [spoofing], you actually have to prove it’s illegal. You might want to look at your algo’.

Despite responses of this kind, the shift from trading pits to electronic order books indeed seems, as Pardo-Guerra (2019b) suggests, to have altered spoofing’s moral status. TC, a former pit trader who became heavily involved in automated trading, suggests that the crucial change was that a bid or offer, formerly inaudible and invisible to those not present in the pit, now ‘goes out on the [electronic] price feed ... the public didn’t see that before. The public didn’t get that piece of information. That’s one change the technology brought about’.

For some HFT interviewees, spoofing was self-evidently illegitimate. There is an ‘obvious line of good and bad’, said TJ: ‘it’s wrong’. Others, pressed by me to explain moral intuitions of this kind, referred to market ideals, especially market efficiency. ‘[I]f you think of the purpose of markets as a price-discovery mechanism, as being efficient’, said TF, ‘then spoofing delays price discovery’. Spoofing is ‘inefficient’, said lawyer LC, when asked by me why he thought it should be illegal. ‘It distorts prices. We want markets to be efficient and accurate at setting prices. You want as few distortions as possible. Spoofing distorts prices in America. That’s why’. Another lawyer, LA, said in my first interview with him: ‘[T]he theory of markets is that it’s like your daily newspaper. There should not be fake news. It’s as simple as that’. In a second meeting he added,

‘The idea of market price is that it’s pure ... bona fide’. A spoofed price is an ‘artificial price’; spoofing ‘conveys a false price to the world’. There should be ‘a purity in market price’, and the latter should reflect the ‘ordinary processes of supply and demand’.

Yet there was a streak of ambivalence in even LA’s views. On a third occasion, he pointed out that few people had reflected in any depth about the legitimacy of spoofing until the Dodd-Frank amendment, and ‘[n]othing has convinced me it’s [spoofing is] so bad’. Some HFT interviewees plainly disagreed with the legal crackdown on the activity. Spoofing is a ‘self-healing problem’, said TK: the algorithmic behaviour that spoofers exploit is ‘very simple and silly ... “I see a bid, I’m going to buy”’. So on balance the market works it out themselves – algorithms can and should be refined so that they are not easily fooled. ‘I saw a quote once’, said TL, ‘that what people call spoofing now, people used to call trading’, and he seemed to agree that spoofing was in this sense ‘normal’ trading behaviour.

The view that spoofing is ‘normal’ seems, however, to have been eroded by the shift from open-outcry pits to electronic order books: when, e.g. TE, quoted above, talked of ‘normal trading’ he was referring to trading *without* spoofing. The risk of criminal prosecution, though, still seemed remote, despite ‘law in books’ that could be read as outlawing spoofing. For example, section 118 of the UK Financial Services and Markets Act, 2000, prohibited conduct that is ‘likely to give ... a false or misleading impression as to the supply of, or demand for, or as to the price or value of, investments of the kind in question’. Yet, Zaloom’s fellow traders in London in autumn/winter 2000 seem not to have known: ‘there was nothing illegal’, she writes, ‘about a Spoofers’ maneuver of supplementing the numbers with the weight of his bid or offer’ (2006, pp. 157–158).

From around 2001 onwards, there was sporadic administrative action against spoofing in US share trading by the SEC and other regulatory bodies. In 2001, the SEC imposed civil penalties totalling just over \$40,000 in aggregate on five traders (SEC, 2001). A decade later, the share-trading firm Trillium agreed a \$1 million spoofing settlement, with 11 employees paying penalties from \$12,500 to \$220,000 and being suspended from securities markets for between six months and two years. The career effects of such a suspension should not be underestimated, but with spoofing being both simple and sometimes highly profitable, administrative penalties could be regarded as worth risking. Jail would be quite another matter, but that did not yet seem likely.

### Law in books, law in action

The process that turned spoofing from a law-in-books to a law-in-action crime began, paradoxically enough, with an episode that had little or nothing to do with spoofing: the global financial crisis of 2008. The crisis sparked temporarily strong Congressional engagement with financial reform. Interviewee LB

reports that a leading Democratic senator (involved in the framing of the main legislative response to the crisis, the Dodd-Frank Act) approached the futures market regulator, the CFTC, asking it to review its existing legal powers to take action against market manipulation. The agency was indeed dissatisfied with these: nearly 30 years previously, it had suffered what interviewee LA calls a ‘devastating’ legal setback when the courts rejected the CFTC’s allegation that a farmers cooperative in Indiana had engaged in market manipulation. After that, says LA, the CFTC rarely brought ‘manipulation cases ... except [in] isolated circumstances’. The legal hurdle – summarized by LA as ‘you have to show an intent to affect a price, the [accused’s] ability to affect the price, and an artificial price as a result’ – was too high.

When the senator’s request arrived, the CFTC had already encountered what interviewee RA calls ‘early examples’ of spoofing in futures markets, and it responded by proposing that the Dodd-Frank Act should insert into the Commodity Exchange Act a specific prohibition on spoofing in futures markets, so that it need not be treated as an instance of more general, hard-to-prove ‘market manipulation’. Interviewee LB was involved in drafting the prohibition, including ‘trying to write the definition for spoofing. An impossible task.’ He worried that any explicit definition would be too narrow, as traders found new ways of spoofing that avoided violating the letter of the law.

The Commodity Exchange Act, though, already banned ‘wash trading’ (‘something else that is impossible to define’, says LB, although it can be thought of loosely as trading that, by design, does not involve any genuine economic exchange) without saying at all explicitly what it was: section 4c of the Act merely prohibited any transaction that ‘is, of the character of, or is commonly known to the trade as, a “wash sale”’. That formulation was therefore simply re-used in the prohibition of spoofing quoted at the start of this paper. Others involved in the drafting, though, seem to have been uncomfortable with having nothing more than the equivalent of the wash-sale wording, and wanted something closer to a definition of spoofing. They prevailed: the 14 words ‘bidding or offering with the intent to cancel the bid or offer before execution’ were inserted within parentheses. The surrounding text (‘is of the character of’, etc.) does, however, preserve some of LB’s intended generality.

‘Intent to cancel’ was a more concrete issue than whether a price was ‘artificial’. Instructions from a trader to a programmer, or a programmer’s notes on a meeting with the trader, might suffice to demonstrate that intent: the burden of proof was less. Nevertheless, the effect of the new legal provision was not initially dramatic. Its first use was in a 2013 administrative action by the CFTC against a small New Jersey futures trading firm, Panther Energy Trading, and its owner Michael Coscia. To begin with, nothing seemed exceptional about the case. The CFTC had already taken a small number of such actions against alleged spoofers, using pre-Dodd-Frank legal provisions (in administrative actions, the standard of proof is not ‘beyond reasonable doubt’ but the civil law’s ‘preponderance of the evidence’). All those accused

eventually agreed a settlement with the CFTC (see the list in Canellos *et al.*, 2016). In July 2013, Mr Coscia and his firm did so too. Without admitting or denying rule breaking, they agreed to pay a civil penalty of \$1.4 million and serve a year's ban from futures trading.

The Department of Justice, responsible for Federal criminal law, had however started to take an interest in spoofing, most likely triggered by the explicit prohibition that now existed. The Department, so interviewee RB tells me, 'reads every [case]' – both CFTC cases and those settled by disciplinary action by an exchange – and sometimes 'does their own investigating'. In April 2014, the US Attorney's Office for the Northern District of Illinois, better known for prosecuting gang violence, organized crime and corruption, had set up a Securities and Commodities Fraud Section, an area previously the domain primarily of the Office for the Southern District of New York. On 2 October 2014, the Northern Illinois Office announced six charges of commodities fraud and six of spoofing against Mr Coscia.

It was a pivotal moment. When I visited Chicago three weeks later, interviewee TF said that the atmosphere in futures trading had changed radically. 'Since that indictment came out', he said, 'the activity [spoofing] has gone way down', which he welcomed. He added, however: 'It's scary too, because anything that appears [like spoofing] you might go to jail for now, so you've got to be really careful'. Like Zaloom's colleagues in London, many futures traders in the United States may not have realized that the law had changed. When news of criminal charges prompted them to read spoofing's legal definition, many felt that the boundary separating it from legitimate trading was unclear (e.g. TC, who had read the definition in 2010, 'just thought it was vague'; he preferred what he regarded as the more explicit wording of the anti-spoofing Rule 575 that the world's leading futures exchange, the Chicago Mercantile Exchange, added to its rulebook in 2014, but that does not have the force of law). Traders worried, e.g. that a stop-loss order might count as spoofing. Such an order automatically liquidates a trading position when prices have moved adversely by a fixed amount. Since its execution crystallizes a loss, traders certainly hope that it will never be executed, and can be cancelled once there is no further need for it.

The change in trading's atmosphere would most likely have been temporary if boundary work of a quite different kind – presenting a prosecution case in front of a jury of laypeople – had failed. The seven-day trial was held in the Dirksen Courthouse in Mies van der Rohe's austere modernist Chicago Federal Plaza. Interviewee RB sat through it, and felt the Northern Illinois prosecutors did their work skilfully. He was struck, e.g. by the homely analogy for the cancellation of orders used by one of the two prosecuting attorneys in his final address to the jury:

You know, it reminds me of something that I used to see on the playground at school ... There was a kid who would put his hand out like this like he was trying to shake your hand, and he'd pull it away right when you were about to shake his

hand ... He thought that was very funny. I didn't.

(US District Court for the Northern District of Illinois,  
Eastern Division, 2015, p. 1547)

One danger to the prosecution was 'a question [that] pops up a lot' (interviewee RA): 'who's really getting hurt? These [HFT] billionaires are losing a couple of bucks here and there'. ('Billionaire' considerably exaggerates the typical profitability of HFT, but a lay jury could not be expected to know that.) The prosecution's four witnesses from HFT firms (and one from a firm specializing in 'statistical arbitrage') were, however, preceded by an agricultural futures trader who described himself as a 'farmer and a rancher' who lived on a '[f]ifth generation family farm' in Kansas, and worked on behalf of JBS, owner of Pilgrim's Pride, a brand well known to US consumers (US District Court for the Northern District of Illinois, Eastern Division, 2015, pp. 607–608).

After a seven-day trial, the jury convicted Mr Coscia, and in July 2016, he was sentenced to three years in jail. An appeal, on grounds of insufficient evidence and the reasoning that the prohibition on spoofing was unconstitutionally vague, was unsuccessful, with the US Court of Appeals for the Seventh Circuit (2017, p. 18) arguing that 'the statute clearly defines "spoofing" in the parenthetical': i.e. in the 14 words in brackets. (Mr Coscia has subsequently pursued other grounds of appeal.) The case was soon followed by another that received much wider publicity, that of the London futures trader Navinder Singh Sarao, whose indictment suggested – controversially (Vaughan, 2020, p. 188) – that his alleged spoofing had contributed to the Flash Crash, 20 minutes of extreme turmoil in the US financial markets on 6 May 2010.

The higher-profile prosecution of Mr Sarao was led by 'Main Justice', the Justice Department's Washington DC headquarters. He was arrested in April 2015 at his parents' modest suburban house (where he still lived and did his trading, despite being in his mid-30s and a successful trader), and detained in London's grim Wandsworth Prison, at one point reportedly saving the life of a cellmate who was trying to hang himself, holding him up by his legs until a warder arrived (Vaughan, 2020, p. 183). When deported to the United States, he was held in Chicago's forbidding skyscraper jail, the Metropolitan Correctional Center. He agreed to cooperate with the prosecution, pleading guilty when he appeared in the Dirksen Courthouse in November 2016, and was eventually sentenced to a year of confinement in his parents' home.

### **The work of drawing a boundary is never done**

By the time of my 2017 visits to Chicago, I found that the crackdown on spoofing in US futures trading had become institutionalized, indeed almost routinized. The pits' relaxed attitudes, lenient treatment in electronic trading's early years, what Williams (2009) correctly describes as the typical situation of financial-market surveillance in which 'advantage ... lies in the hands of

the watched rather than the watchers' (p. 485) – all these belonged in a different epoch. Now, TF told me, there was often no need for a trading firm to complain about spoofing, as there had been even three years previously. The exchanges had developed software systems that detected it quickly: 'I would be very surprised if a large spoofer went undetected for more than a couple of days. ... They're catching the spoofer ... fining him \$25,000, kicking them out of the market', and doing that regularly, with cases reported almost weekly. As another HFT interviewee, TM, confirmed, spoofing had indeed become 'less of a problem'.

Asked by me to explain the change, TF gave a one-word answer: 'Coscia'. He went on: 'I think someone going to jail changed the attitude, that's what it comes down to'. An exchange could not afford leniency: 'if someone is going to jail for it, and they're not doing anything about it, it looks terrible'. The process he described could be thought of as almost Durkheimian: the treatment of an act as a crime, and its punishment by jail, had crystallized what had been an ambivalent, contested moral divide, turning it into what appeared, at least at first sight, to be a clear boundary, policed by machines (automated spoofing detection systems), not just human beings.<sup>3</sup>

For at least two reasons, though, that conclusion would be over-simple. First, law and morality continue to interact. As LC puts it, a jury *should* make 'factual judgements', but in practice a prosecutor needs to do more than show that the accused 'has broken the law within the technical definition of it'. '[Y]ou're asking [a jury] to make a moral judgement: that this person is a criminal and they're worthy of being called a criminal'. The jury, he says, will ask themselves: 'was he *in on it*'?

The next contested spoofing case to reach Chicago's Dirksen Courthouse, in April 2019, involved an attempt to expand the legal boundary: to prosecute not a trader who had allegedly spoofed, but a programmer, Jitesh Thakkar, whose firm (Edge Financial Technologies) had written software allegedly used by the trader. With the trader, Navinder Singh Sarao, called as a prosecution witness, Thakkar's defence team was led by one of the Northern Illinois prosecutors of Michael Coscia. Interviewee RB, who had sat through the latter's trial, saw Mr Thakkar's attorney show the defence's first exhibit to the court. Two simple lines of text appeared on the courtroom's screens, with, 'in big font', an estimate of what Sarao's trading had earned him (RB remembers the figure as \$39 million), and 'right under that ... in really small letters' the amount that Thakkar's firm was said to have earned by allegedly writing the software in question (\$24,000, he recalls). At that moment, RB realized that the prosecution would fail: whatever the software had been used for, Mr Thakkar was clearly not morally 'in on it'. He was indeed acquitted.

That criminal law's boundary-drawing thus remains moral work has material consequences. The Dodd-Frank definition of spoofing involves the spoofer *intending* to cancel orders. It would be hard, warns LC, to persuade a jury to take the morally weighty decision to convict someone of a crime on the basis of just 'the statistics and the data' of trading patterns. '[Y]ou need to have



very clear evidence of intent', he says, and in practice that means evidence that takes material form: 'either ... emails, text messages, handwritten notes [or] an algorithm that in itself [in] the programming indicates an intent to cancel'.

Second, definitions do not unequivocally bisect the world. For example, the Dodd-Frank definition of spoofing involves *cancelling* orders. Cancellation usually means a user or an algorithm sending an electronic message to an exchange's system instructing the latter to cancel an order. But there are at least two other ways to achieve a similar effect. One is by using the 'self-matching' prevention mechanism in the software of many exchanges, including the Chicago Mercantile Exchange. Most trading firms operate several (perhaps many) different algorithms, and one of them can accidentally send in an order that would execute against another's pre-existing order, which could constitute illegal 'wash trading'. The self-matching prevention mechanism instead cancels both orders. That allows a spoofer to 'cancel without cancelling', by sending in a new order that causes the self-matching prevention mechanism to cancel the original spoof order. Another way in which a spoofer can avoid actually cancelling an order is to send in a message increasing that order's size. The exchange's system will then treat the 'modified-up' order as a new order, and move it to the end of the queue for electronic execution, thus reducing the risk that it will be executed.

A prosecutor who knows how to keep things simple for a jury need not be derailed by a spoofer's use of an exchange's 'self-matching' prevention mechanism, said LC:

I would have just had a human being up there [testifying], explaining that this is a technology that enables you to cancel faster. It doesn't matter what it is, or how it works ... it's something special that allows you to cancel fast. And that's all it is, and let him [the defendant] have a complicated story of explaining that it's something else.

He warned, however, that whether use of the second mechanism, 'modify-up', is equivalent to cancelling an order 'has never been litigated'. That legal uncertainty might tempt a prosecutor to rely not on the 14-word Dodd-Frank definition of spoofing but on the clauses surrounding it ('is of the character of', etc.), but that too could be risky. Because the appeal court invoked the 14-word definition in rejecting the argument that the prohibition on spoofing was unconstitutionally vague, a prosecution that went beyond that definition might face renewed challenge on grounds of 'vagueness'.

Such potential difficulties are not absolute barriers: spoofing can, for example, be prosecuted successfully using the older, less 'technical', law of fraud ('the fraud statute was written over a 100 years ago. It's very broad', says LC). But it is significant that they are only *potential* difficulties. The legal status of use of the self-matching prevention mechanism or 'modify-up' has not so far been a central issue in a contested criminal prosecution.<sup>4</sup> Many cases are still settled by an agreed civil penalty.

In the background to this is an important issue. Like market surveillance more generally (Williams 2009, 2012), boundary work concerning spoofing is indeed work, in a mundane sense. It takes effort and costs money, beginning with alerts from spoofing detection systems that require scrutiny by human beings. Interviewee EB says that even at his relatively small exchange, his colleagues ‘trawl through hundreds of alerts per day, and of course the lion’s share of those are false positives’. Yet more effort is needed if a government regulatory body decides to investigate. ‘Gathering [evidence], travel, interviewing. There’s a lot of sums of money that are being expended’, says former regulator, RC. This affects which cases are pursued: ‘You always had to figure out where your best bang for the buck was going to be’. There is a *de facto* incentive, says interviewee RB, ‘to pursue simple cases, not complex ones’, because they are ‘easier to win’.

If a complex case goes to court, expert witnesses will typically be required to trawl through huge volumes of data. ‘Those experts’, says RB, ‘they give you a discount for working for the government usually, and they’re still \$600–\$700 an hour, and those guys do a lot of work. If you’re going to go down the route of using an expert in a statistical heavy case, that’s expensive’. As LC puts it, white-collar crime is typically ‘[c]omplicated. There’s typically very limited resources to pursue those kind of crimes. There’s a lot of times more emphasis on violent crimes or narcotics...’. At root, the question of resources is a matter of societal priorities, and ultimately an issue of political economy: law in action is indeed not an autonomous sphere.

## Conclusion

Restricted resources thus continue to limit the scope of the crackdown on spoofing, even in US futures trading, as does LC’s point, discussed in the previous section: that, for most juries, criminal culpability is morally too weighty a decision to make without material evidence of ‘intent’ such as an incriminating email. The crackdown seems nevertheless to have influenced conduct in futures trading substantially. Fewer cases of spoofing seem to be being reported, although my interviewees appear reluctant to conclude that it has been eliminated.

‘Did it [spoofing] go away’, asks TN, ‘or is it your ability to detect it, as they become more sophisticated? I don’t know’. TE reports: ‘We’re more finding that spoofing adjusts to make sure it doesn’t hit formal guidelines of what spoofing is’. One possible issue is that exchanges’ detection systems seem to monitor, singly and in combination, levels of (and changes in) parameters such as the ratio of trades to orders, and traders may have learned roughly the ‘trigger values’ that cause an alert. But that would still imply a major influence of the crackdown, because trading that is constrained by the need to avoid trigger values is likely to be quite different from trading without that constraint.

This paper has presented a processual analysis of the crackdown. The general factors identified by Arnoldi and Pardo-Guerra – the vulnerability of HFT algorithms; the ‘moral technology’ of the order book – may be necessary preconditions, but they are not sufficient to explain what has only ever been a partial crackdown (interviewees report, e.g. little action against spoofing in the market for Treasuries, even though these are the sovereign debt securities of the United States). Contingencies have played an essential role, in particular the Congressional request to the CFTC to consider increasing its powers to act against market manipulation, which led to the pivotal Dodd-Frank amendment specifically outlawing spoofing in futures markets.

What is being cracked down on – spoofing – is not a unitary, unambiguously defined activity. Traders did informally distinguish spoofing from other forms of electronic trading prior to the organized boundary work triggered by the Dodd-Frank amendment, but they did so in variable ways. Nor has that boundary work led to a fully definitive way of separating spoofing from legitimate trading: the complications of ‘self-matching prevention’ and ‘modify-up’ show that applying the Dodd-Frank definition may continue to require further, potentially contestable, boundary work. Indeed, if the finitist sociology of, e.g. Barnes and Bloor is correct, we should not expect any such boundary *ever* to be drawn definitively.

There is no inherent inevitability to how spoofing is currently distinguished from legitimate trading in US futures markets: alternatives exist. Recall, e.g. the trader, in the pre-recorded detection-system demonstration, who was selling, but had also placed a large bid to buy. In US futures, trading in this way would almost certainly be classed as spoofing. Four months later, TO (who trades Treasuries, not futures) showed me, this time in live electronic trading, on-screen traces that he interpreted very similarly: a trader placing a large offer to sell while actually wanting to buy. TO’s reaction was, however, quite different: he viewed it as legitimate. ‘[T]hat’s not spoofing’, he said, because the trader did not cancel the offer immediately. ‘You [do] not want to sell, but you leave the offer out there, that’s not spoofing. It’s when ... you flash it [enter the offer, then immediately cancel it], that’s spoofing’. He was drawing the boundary marking out spoofing more narrowly than in the Dodd-Frank amendment, in which the intended cancellation need not happen straightaway. Dodd-Frank’s more expansive approach, though, has informed automated spoofing detection systems and been invoked in criminal prosecutions; TO’s is simply a local, informal cultural understanding.

Different outcomes of this sort cannot be understood without looking beyond the direct activities of trading. In areas such as this, I would argue, we need to take the law more seriously than has often been the case in, for example, analyses of finance inspired by science and technology studies (including some of my own previous work). Mobilization of the criminal law was crucial to the process analyzed here. It had, most obviously, a deterrent effect, but in a way that I have described as almost Durkheimian, it also solidified attitudes, especially within exchanges, turning a loose sense that spoofing was morally wrong (along with

variable understandings of what it was, and inconsistent enforcement) into much more active and increasingly automated surveillance.

Yet, the crucial change in ‘law in books’ – the Dodd-Frank amendment – was nuanced in its effects. Arguably, its importance was less in its ‘technical’ role in prosecutions (older, more general law can be and has been used, even in US futures trading; in other markets, both in the United States and internationally, less specific law is also available, even if it is not being used in criminal prosecution), than in the Dodd-Frank amendment’s naming of spoofing and specific outlawing of it. Certainly, a group of regulators and surveillance specialists in a European country that has law in books that could be used to prosecute spoofing, but no equivalent specific ban, told me they very much wished that such a ban existed in their jurisdiction.

Just as Riles (2010) argues, law matters. ‘Law in action’ is an apparatus in the fullest sense. It includes automated spoofing detection systems, prosecutors’ ambition or (over)caution (Eisinger, 2017), well-remunerated expert witnesses making sense of data, defendants’ financial and cultural capital (or lack thereof), lawyers’ courtroom skills, the moral reasoning of juries, and ultimately Wandsworth Prison (originally laid out, as Foucault might have anticipated, as a Benthamite panopticon) and the Metropolitan Correctional Center. As I have noted, the prominence specifically of criminal law in the crackdown on spoofing makes it untypical of the regulation and surveillance of finance. But the underlying general issues – boundary work and the interweaving of moral distinctions, legal rules and the material forms taken by economic exchange – are pervasive, perhaps in all markets.

Researchers on markets who work within or are influenced by science and technology studies are persistently criticized for appearing to ignore ‘context or politics’, thus painting a picture that is ‘all cogs and no car’ (Chakraborty, 2012). Such researchers are often reluctant – rightly so, in my view – to invoke notions of power and social structure (or even simply ‘context’) that lack a grounding in their fieldwork. Yet, if we do not trace the connections between intricate technical domains such as mathematical modelling or HFT and broader issues of culture and political economy, then criticisms such as Chakraborty’s (2012) are valid. Finding a way of doing that while remaining faithful to broadly ethnographic research methods is, however, not always easy.

Attention to law offers a promising approach, as the example of spoofing shows. On the one hand, the prohibition of spoofing has clear, concrete effects on HFT. It constrains how HFT algorithms can act; influences how HFT algorithms analyze order books; and enables forms of HFT that might otherwise succumb to spoofing to be at least modestly successful. On the other hand, the criminalization of spoofing exemplifies a more general change in law diagnosed by Farmer (*in press*): from protecting market participants and other individuals from specific harms such as fraud, to protecting the market itself and its ‘integrity’. (Note that the Dodd-Frank prohibition does not require that any participant suffer a loss from the prohibited activity.)

Changes of this kind in law are often connected to wider cultural shifts, such as changing views of markets. (As Farmer suggests, the changed legal approach is

connected to the efficient market hypothesis having escaped the lecture theatres and spread in the wider culture, especially in the United States: recall how my interviewees cited ‘efficiency’ when asked why spoofing should be illegal.) Placing law at the centre of our analytical attention could thus help us in an essential task – tracing the connections between the market devices that we research in depth and the wider cultures and political economies of which they form part.

### **Acknowledgements**

Huge thanks are due to my interviewees.

### **Disclosure statement**

No potential conflict of interest was reported by the author(s).

### **Funding**

Funding was received from the UK Economic and Social Research Council [grant numbers ES/R003173/1 and RES-062-23-1958] and European Research Council [grant number 291733].

### **Notes**

- 1 By late 2020, 21 individuals and five corporate bodies had faced US criminal charges for spoofing (Ray *et al.*, 2020). Two allegations concern share trading; part of another case, against JP Morgan Chase, concerns Treasuries, US government debt securities. All other cases concern futures.
- 2 To help preserve anonymity, codes employed here differ from in MacKenzie (2021).
- 3 See, e.g., Durkheim [2013 (1893), p. 79].
- 4 A contested civil hearing involved a trader’s alleged use of self-matching prevention, but its status was not central to the hearing (US District Court for the Northern District of Illinois, Eastern Division, 2016). The Sarao case involved modify-up, but was settled by his guilty plea.

### **ORCID**

Donald MacKenzie  <http://orcid.org/0000-0002-1860-8116>

## References

- Arnoldi, J. (2016).** Computer algorithms, market manipulation and the institutionalization of high frequency trading. *Theory, Culture & Society*, 33(1), 29–52.
- Barnes, B., Bloor, D. & Henry, J. (1996).** *Scientific knowledge: A sociological analysis*. Athlone.
- Canellos, G. S., Rangwala, T. S., Walfish, D. R., Jou, J. K. & Palladino, S. L. (2016).** *The law surrounding spoofing in the derivatives and securities markets*. Retrieve from <https://www.milbank.com/images/content/2/4/v5/24678/Spoofing-in-the-Derivatives-and-Securities-Markets-June-2016.pdf> [Accessed 27 November 2017].
- Chakraborty, A. (2012).** *Economics has failed us: But where are the fresh voices?* Retrieve from <https://www.theguardian.com/commentisfree/2012/apr/16/economics-has-failed-us-alternative-voices> [Accessed 6 August 2021].
- Coombs, N. (2016).** What is an algorithm? Financial regulation in the era of high-frequency trading. *Economy and Society*, 45(2), 278–302.
- Durkheim, E. (2013 [1893]).** *The division of labour in society*. Palgrave Macmillan.
- Eisinger, J. (2017).** *The chickenshit club: Why the Justice Department fails to prosecute executives*. Simon & Schuster.
- Farmer, L. (in press).** The ‘market’ in criminal law theory. *Modern Law Review*.
- Fourcade, M. & Healy, K. (2007).** Moral views of market society. *Annual Review of Sociology*, 33, 285–311.
- Gieryn, T. F. (1983).** Boundary-work and the demarcation of science from non-science: Strains and interests in professional ideologies of scientists. *American Sociological Review*, 48(6), 781–795.
- Greising, D. & Morse, L. (1991).** *Brokers, bagmen, and moles: Fraud and corruption in the Chicago futures markets*. Wiley.
- Grundfest, J. A. (1989).** *Integrity and competition in Chicago’s futures markets*. Retrieve from <https://www.sec.gov/news/speech/1989/101289grundfest.pdf>, [Accessed 23 April 2021].
- Halpérin, J.-L. (2011).** Law in books and law in action: The problem of legal change. *Maine Law Review*, 64, 46–76.
- Lamont, M. (2000).** *The dignity of working men: Morality and the boundaries of race, class, and immigration*. Harvard University Press.
- Lenglet, M. (2011).** Conflicting codes and codings: How algorithmic trading is reshaping financial regulation. *Theory, Culture & Society*, 28(6), 44–66.
- Lenglet, M. & Mol, J. (2016).** Squaring the speed of light? Regulating market access in algorithmic finance. *Economy and Society*, 45(2), 201–229.
- MacKenzie, D. (2006).** *An engine, not a camera: How financial models shape markets*. MIT Press.
- MacKenzie, D. (2021).** *Trading at the speed of light: How ultrafast algorithms are transforming financial markets*. Princeton University Press.
- Milyaeva, S. (2013).** Tipping the balance: Russian legal culture and cash-settled derivatives. *Journal of Cultural Economy*, 7 (2), 209–225.
- Pardo-Guerra, J. P. (2019a).** *Automating finance: Infrastructures, engineers, and the making of electronic markets*. Cambridge University Press.
- Pardo-Guerra, J. P. (2019b).** What is a ‘real’ transaction in high-frequency trading. In F. Neiburg & J. I. Guyer (Eds.), *The real economy: Essays in ethnographic theory* (pp. 103–127). Hau.
- Pound, R. (1910).** Law in books and law in action. *American Law Review*, 44, 22–36.
- Ray, J. L., Sharp, N. & Welland, J. (2020).** *Spoofing and market manipulation: 2020 year in review*. Retrieve from <https://www.rahmanravelli.co.uk/articles/spoofing-and-market-manipulation-2020-year-in-review/> [Accessed 13 April 2021].
- Riles, A. (2010).** Collateral expertise: Legal knowledge in the global financial

- markets. *Current Anthropology*, 51(6), 795–818.
- SEC.** (2001). SEC charges six individuals with spoofing. Retrieve from <https://www.sec.gov/news/press/2001-129.txt> [Accessed 6 August 2021].
- US Court of Appeals for the Seventh Circuit.** (2017). *No. 16-3017: United States of America v. Michael Coscia*. Retrieve from <http://law.justia.com/cases/federal/appellate-courts/ca78/16-3017/16-3017-2017-08-07.html> [Accessed 5 October 2017].
- US District Court for the Northern District of Illinois, Eastern Division.** (2015). *No. 14 CR 00551: United States of America v. Michael Coscia. Transcript of proceedings*. Access provided by interviewee.
- US District Court for the Northern District of Illinois, Eastern Division.** (2016). *No. 15 CV 9196: US Commodity Futures Trading Commission v. Igor B. Oystacher and 3Red Trading LLC*. Retrieve from [https://www.govinfo.gov/content/pkg/USCOURTS-ilnd-1\\_15-cv-09196/pdf/USCOURTS-ilnd-1\\_15-cv-09196-2.pdf](https://www.govinfo.gov/content/pkg/USCOURTS-ilnd-1_15-cv-09196/pdf/USCOURTS-ilnd-1_15-cv-09196-2.pdf) [Accessed 18 May 2021].
- Vaughan, L.** (2020). *Flash crash: A trading savant, a global manhunt and the most mysterious market crash in history*. Collins.
- Williams, J. W.** (2009). Envisioning financial disorder: Financial surveillance and the securities industry. *Economy and Society*, 38(3), 460–491.
- Williams, J. W.** (2012). *Policing the markets: Inside the black box of securities enforcement*. Routledge.
- Zaloom, C.** (2006). *Out of the pits: Trading and technology from Chicago to London*. Chicago University Press.
- Zelizer, V. A.** (2012). How I became a relational economic sociologist and what does that mean? *Politics & Society*, 40(2), 145–174.
- US legislation cited**
- Commodity Exchange Act*. US Code Title 7, Agriculture. Chapter 1: Commodity Exchanges. Retrieve from <https://www.law.cornell.edu/uscode/text/7/chapter-1> [Accessed 21 April 2021].
- Dodd-Frank Wall Street Reform and Consumer Protection Act*. Public Law 111-203, 21 July 2010. Retrieve from <https://www.congress.gov/111/plaws/publ203/PLAW-111publ203.pdf> [Accessed 22 April 2021].
- UK legislation cited**
- UK Financial Services and Markets Act, 2000*. Retrieve from <https://www.legislation.gov.uk/ukpga/2000/8/contents> [Accessed 21 April 2021].

**Donald MacKenzie** teaches sociology at the University of Edinburgh. His most recent book is *Trading at the speed of light: How ultrafast algorithms are transforming financial markets* (Princeton University Press, 2021).