

RESEARCH ARTICLE

The industrialisation of fraud: understanding fraud in a digital era

Jennifer Collins[†] 

University of Bristol, Bristol, UK
Email: jennifer.collins@bristol.ac.uk

(Received 06 April 2025; revised 28 October 2025; Accepted 29 October 2025)

Abstract

This paper offers a novel conceptual framework for understanding fraud in the digital era by introducing the idea of industrialised fraud. Unlike existing literature that focuses on the mechanics of cyber-enabled and cyber-dependent fraud, this work situates fraud within the social, structural, technological and economic transformations of the digitalised economy. It argues that fraud is no longer an outlier but a systemic feature of unregulated digital markets, operating at scale and across borders. Through the analytical lenses of fraud's footholds and fraud's lifecycles, the paper reexamines fraud's core legal and moral norms – means, purposes and fault. It demonstrates how they are being reshaped by the transactional contexts in which fraud is now designed, facilitated and perpetrated. This reconceptualisation provides a firmer foundation for principled debate on fraud governance and criminalisation in an era of rapid technological transformation.

Keywords: criminal law; fraud; industrialised fraud; digitalised economy; Fraud Act 2006; emerging technologies

Introduction

Fraud is a pervasive global problem which causes widespread economic and psychological harm to victims. It can be spontaneous or planned by skilful organised crime groups.¹ Increasingly fraud is facilitated across borders by advances in innovative technologies, including artificial intelligence, large language models, social engineering and cryptocurrencies.² Nationally, the problem of fraud in England and Wales has reached a crisis point; fraud is now the most common crime experienced by victims in England and Wales and accounts for approximately 37% of all crime.³ The economic value of reported fraud over £50,000 in England and Wales in 2023 was estimated to be £2.3 billion.⁴

This paper argues that it is now time to revisit the meanings of fraud, in part prompted by considerable policy and legal attention on fraud criminalisation and governance in England and Wales.⁵ It is also reasonable to suspect that the concept of fraud has shifted with technological change – affecting

[†]Associate Professor in Law, University of Bristol. I am very grateful to Andrew Ashworth, Alan Bogg, Bob Sullivan, participants at the Oxford Criminal Law Discussion Group and two anonymous reviewers for incisive comments on drafts.

¹UNODC *Organized Fraud: Issue Paper* (Vienna, 2024) p 9.

²*Ibid*, pp 55–57.

³ONS *Crime in England and Wales: Year Ending September 2024* (2025).

⁴BDO UK *FraudTrack 2024* (2024), from 1 December 2022 to 30 November 2023.

⁵House of Commons Justice Committee *Fraud and the Justice System* Fourth Report of Session 2022–23, HC12, 18 October 2022 (HMSO, 2022); House of Lords Fraud Act 2006 and Digital Fraud Committee *Fighting Fraud: Breaking the Chain* Report of Session 2022–23, HL 87, 12 November 2022 (HMSO, 2022); Home Office *Fraud Strategy: Stopping Scams and Protecting the Public* CP 839 (May 2023).

its scale, nature and how it is defined and prosecuted under the law.⁶ Since fraud is pervasive, prevalent and growing, it is important that we have a detailed conceptual understanding of fraud prior to discussions about fraud criminalisation, prevention and associated regulatory strategies.⁷ It is easy, given fraud's ubiquity and the frequency with which fraud is talked about, to assume that we know what we mean by it. However, the issue of fraud's conceptual foundations is rarely addressed directly in criminal law literature.⁸

As I will explain, there is broad consensus around the identification of fraud's core norms and this paper does not challenge their relevance. These include deliberately taking dishonest advantage of another person, often by false representation; failure to disclose information; and abuse of a position of trust, for financial purposes. Rather, this paper argues that the context in which fraud's core norms operate – namely, the digitalised economy – has received insufficient theoretical attention.

This paper proceeds in four parts. The first section lays the groundwork by advancing a contextual approach to unpacking fraud's meanings. The second section develops the paper's core conceptual framework, arguing that the digitalised economy must now be central to theorising fraud in the twenty-first century. It introduces the concept of *industrialised fraud* – fraud embedded at scale and across borders within digital infrastructures – and within this, the notion of *fraud's footholds*. The latter are the structural features of the digitalised economy which shape fraud. The third section presents *fraud's lifecycles* – the temporal stages of fraud (approach, interaction and outbound) – as a further analytical tool to understand how fraud is designed, implemented and experienced in the digitalised economy. It shows how fraud's footholds and lifecycles in the digitalised economy are reshaping fraud's core legal and moral norms, particularly in relation to fraud's means, purposes and fault. The final section argues that this reconceptualisation provides a firmer foundation for future work on fraud criminalisation and regulation.

Two preliminary disclaimers are needed. The conceptual work undertaken in this paper is directed towards those seeking to understand 'fraud' better for the purposes of criminal law. It will be of interest to criminal lawyers, theorists and practitioners seeking to put debates about fraud criminalisation and connected regulatory strategies on a surer footing. It is for other work to consider the meanings of fraud with specific relevance to civil law. Secondly, this paper focuses on fraud while acknowledging that in theory and practice it is difficult to separate out fraud from its place within economic crime. In practice, fraud can be used as a means of facilitating other organised crimes, such as money laundering or trafficking of people and goods.⁹ There is more work to be done on economic crime as part of the 'Special Part' of the criminal law.¹⁰ Given the current legal importance of fraud, it is argued that a detailed study of fraud is a compelling place to begin.

1. Unpacking fraud contextually

This section interrogates how criminal lawyers and theorists ought to unpack fraud's meanings. This task is separate from, and a precursor to, arguments about the appropriate contours of criminalisation and associated regulatory interventions. It is also distinct from attempts to assign non-legal labels of 'fraud' to transactions or persons that appear suspect.¹¹

⁶Europol ChatGPT: *The Impact of Large Language Models on Law Enforcement* (Luxembourg: Publications Office of the European Union, 2023).

⁷Cifas *Fraudscape* 2024 (2024) https://assets-global.website-files.com/5f24212f91518a2cd44d736f/661e5650fdbfbcc31e8ab3c6_Cifas%20Fraudscape%202024%20Downloadable%20Report.pdf.

⁸A failure to define fraud characterised implementation of the Fraud Act 2006: see D Ormerod 'The Fraud Act 2006 – criminalising lying?' [2007] *Criminal Law Review* 193 at 195.

⁹Europol *European Union Serious and Organised Crime Threat Assessment, A Corrupting Influence* (EU SOCTA, Publications Office of the European Union, 2021) p 76.

¹⁰See RA Duff and S Green (eds) *Essays on The Special Part of the Criminal Law* (Oxford: Oxford University Press, 2005).

¹¹A person can be described as a 'fraud', or a person can commit 'fraud'. For a popular media example, see *The Tinder Swindler* (Netflix, 2022) <https://www.netflix.com/gb/title/81254340>.

The basis of my argument is that unpacking fraud's meanings for those interested in the criminal law now needs to push beyond current legal and moral framings in criminal law literature. As I will explain, there are two dominant approaches in this literature. First is a focus on unpacking fraud's meanings in the context of specific fraud offences which form part of the 'Special Part' of the criminal law. The second is to interrogate fraud's meanings through examination of fraud's moral foundations. Using Lindsey Farmer and Nicola Lacey's seminal work identifying the criminal law as a public institution, I argue that enquiry into fraud's meanings needs to be grounded in the transactional context in which frauds are now facilitated and perpetrated.¹² We cannot understand fraud's meanings without unpacking the concept within its surrounding, dominant, normative context – a task which has not yet been undertaken. The specifics of the relevant context are identified and examined in this paper's third section, below.

(a) Existing criminal law literature on fraud's meanings

We see two trends in how contemporary criminal law theory has addressed unpacking fraud's meanings. The first approach delineates fraud's meanings through the prism of existing offences. While many offences target fraud in statutes and at common law in England and Wales, in this literature fraud's meanings are closely related to the approach taken to fraud in sections 1–4 of the Fraud Act 2006.¹³ The section 1 fraud offence sets out a basis for establishing criminal liability, identifying that fraud can be committed in one of three ways. The section 1 offence does not offer a definition of 'fraud'.¹⁴ Rather, the accompanying sections 2–4 set out three ways of committing the section 1 fraud offence: by false representation; failure to disclose information; or abuse of a position of trust. What is central to the section 1 offence is dishonest intent to gain or to cause loss or the risk of loss through one of the specified forms of conduct. This is an expansive offence, drafted in inchoate mode. An inchoate offence is preventive in that it penalises conduct which has not yet caused a harmful wrong.

In line with the purpose of leading criminal law texts to expound core criminal law offences for their readership, fraud is analysed through the prism of the section 1 fraud offence (and surrounding offences) in *Ashworth's Principles of Criminal Law*, *Simester and Sullivan's Criminal Law: Theory and Doctrine*, and *Smith, Hogan, and Ormerod's Criminal Law*.¹⁵ Simester and Sullivan's seminal textbook emphasises the significant real-world challenge of 'high-volume, relatively low-value fraud' as 'one of the uglier defining features of our time'.¹⁶ There is further helpful elaboration of fraud's relationship to property interests and manipulation/exploitation of victims of fraud.¹⁷ Despite acknowledgment that section 1 of the Fraud Act 2006 does not define fraud, the onus of core texts is on elaborating fraud using the model of criminal liability presented in the section 1 offence.

It is similarly common to find reliance on the section 1 general fraud offence as providing the 'meaning' of fraud for the purposes of policy work on fraud. For example, Policy Exchange's report on fraud identifies the Fraud Act 2006's section 1 offence as the 'definition of fraud'.¹⁸ The Home Office, which holds overall responsibility for fraud, allocated one paragraph to outlining fraud's meaning in the ten-year *Fraud Strategy*, relying upon the section 1 presentation.¹⁹ Full reliance was also placed on the

¹²L Farmer *Making the Modern Criminal Law* (Oxford: Oxford University Press, 2016); N Lacey *In Search of Criminal Responsibility: Ideas, Interests, and Institutions* (Oxford: Oxford University Press, 2016).

¹³Sitting alongside Computer Misuse Act 1990 offences, false accounting (Theft Act 1968, s 17), the Proceeds of Crime Act 2002 and the common law offence of conspiracy to defraud.

¹⁴Mirroring the approach adopted in the Law Commission's *Fraud and Deception* Law Com No 276 (2002).

¹⁵J Horder *Ashworth's Principles of Criminal Law* (Oxford: Oxford University Press, 10th edn, 2022); AP Simester et al *Simester and Sullivan's Criminal Law: Theory and Doctrine* (Hart Publishing, 8th edn, 2022); D Ormerod et al *Smith, Hogan, and Ormerod's Criminal Law* (Oxford: Oxford University Press, 17th edn, 2024).

¹⁶*Simester and Sullivan's Criminal Law: Theory and Doctrine*, *ibid*, p 706.

¹⁷*Ibid*, p 706.

¹⁸R Walton et al *Daylight Robbery: Uncovering the True Cost of Public Sector Fraud in the Age of Covid-19* (London: Policy Exchange, 2020) p 19.

¹⁹See above n 5, p 9.

2006 Act's presentation of fraud in the House of Commons and House of Lords' recent Committee reports on fraud.²⁰ Reliance on a broad account of fraud provides scope to encompass new innovations.²¹ It also provides scope to ask whether conduct is threatening to individual or collective interests.²²

Secondly, we see fraud's meanings addressed through unpacking fraud's connected moral meanings. Fraud is explained by the Crown Prosecution Service as: 'the act of gaining a dishonest advantage, often financial, over another person'.²³ Action Fraud adds the concept of 'trickery' (linked to deceit) to this formulation: fraud is 'when trickery is used to gain a dishonest advantage, which is often financial, over another person'.²⁴ Jeremy Horder's leading criminal law textbook ties fraud's meaning to the broader landscape of corporate criminal activity.²⁵ Specifically, Horder highlights fraud as a form of financial crime which is animated by breach of trust.²⁶ Trust is elaborated according to political economist Francis Fukuyama's account of 'regular, honest, and cooperative behaviour, based on commonly shared norms' in a community.²⁷ These accounts articulate a paradigm in which fraud involves dishonest breach of trust; deception and/or trickery; alongside intent to gain/cause loss or the risk of loss.

The leading legal-philosophical account of fraud's moral foundations is provided by Stuart Green in his monograph, *Lying, Cheating and Stealing*.²⁸ Starting with the insight that fraud can reflect 'a protean and proliferating range of meanings' in criminal law, Green argues that fraud offences are informed and shaped by a pre-legal moral norm prohibiting deceit.²⁹ The salient concept of deception incorporates analytically distinct wrongs of lying, misleading, falsely inculpating and falsely exculpating.³⁰ Green's analysis casts important light on how existing fraud offences might track widely understood moral norms. Nevertheless, it assumes that animating pre-legal moral norms can be delineated, and that criminal offences should 'be targeted at an antecedent moral wrong'.³¹ Mitchell Berman has argued that analysis of the moral content of white-collar offences is insufficient without considering too the issue of whether conduct is harmful, otherwise harm prevention measures cannot be adequately explained.³²

Two important insights can be gleaned from these approaches to unpacking fraud and are animating ideas for the work undertaken in this paper. First is the framing of fraud as a process rather than as requiring a result or an outcome. The focus of the Fraud Act 2006's fraud offence is on fraudulent conduct, undertaken with dishonest intent. There is no need for economic interests to be infringed or for victims to believe fraudulent misrepresentations. In practice outcomes are likely to inform a finding of 'fraud'. 'I have been defrauded' may be the initial – perhaps the only – impetus to reporting suspected fraud. However, the focus of process-based accounts is on the means used alone and on an accompanying limited set of means, which may include false representation, failure to disclose or abuse of position.

Secondly, while a fixation on defining 'fraud' is distracting, adopting a 'central case methodology', we can identify a set of fraud's core norms, which include moral ideas.³³ The core norms which underlie 'fraud' are deliberate and dishonest conduct, undertaken to gain or cause loss. Intended gains or losses

²⁰See *Fighting Fraud*, above n 5, HL 87, pp 127–129.

²¹See Ministry of Justice *Post-Legislative Assessment of the Fraud Act 2006* CP 680 (2022) p 14.

²²H Wood et al *The Silent Threat: The Impact of Fraud on UK National Security* (London: RUSI, 2021) p 2. The perceived threat against individuals is encapsulated within *Fraud Strategy*, above n 5, p 3, which characterises fraud in emotive language: '[F]raudsters are becoming more devious'; 'ruthless criminals'; 'cold-hearted crimes'; 'heart-rending cases'.

²³Crown Prosecution Service 'Fraud and economic crime' <https://www.cps.gov.uk/crime-info/fraud-and-economic-crime>.

²⁴Action Fraud 'What is cyber crime and fraud?' <https://www.reportfraud.police.uk/what-is-fraud/>.

²⁵Horder, above n 15, p 455.

²⁶*Ibid*, p 456.

²⁷F Fukuyama *Trust: Social Virtues and the Creation of Prosperity* (New York: The Free Press, 1996) p 26, noted in Horder, above n 15, p 456; Home Office *Fraud Strategy*, above n 5, p 9: 'A fraud involves an act of dishonesty, normally through deception or breach of trust, with intent'.

²⁸SP Green *Lying, Cheating, and Stealing: A Moral Theory of White-Collar Crime* (Oxford: Oxford University Press, 2007).

²⁹*Ibid*, p 148.

³⁰*Ibid*, p 76.

³¹M Berman 'On the moral structure of white collar crime' (2007) 5 *Ohio State Journal of Criminal Law* 301 at 316.

³²*Ibid*, at 320–321.

³³HLA Hart *The Concept of Law* (Oxford: Oxford University Press, 2nd edn, 1994) p 131.

may be financial, but not exclusively. These gains and losses may be actualised in the real world, but this is not necessary. Fraudulent conduct is further animated by a breach of trust.³⁴ This may be through breach of a general duty to operate with truthfulness or may operate within breach of the expectations of a particular trust relationship. Concepts of deliberateness and dishonesty are strongly linked to objective assessments of breach of trust.³⁵ Fraud is facilitated by a set of means, which are used to breach trust. These may include deception, false representations, lack of corrections of untruths, failing to disclose relevant information and misuse of a position of trust.

(b) Contextualising fraud as a criminal wrong

This section further develops these insights. Drawing on and developing Lindsay Farmer and Nicola Lacey's work in contextualising the criminal law, I argue that we need to contextualise the trajectory of criminal wrongs and that this is central to elucidating fraud in contemporary criminal law literature.

The first step in this argument is to move beyond liberal criminal law's focus on moral philosophy as a means of explicating criminal wrongs. A critically important literature recognises that the criminal law is an 'irreducibly political institution, shaped by social and economic interest groups and used by states and governments to enforce social inequalities'.³⁶ This forces attention on criminal law's aims and objectives, identifying the criminal law as an 'institutional normative order'.³⁷ For example, Lacey's sophisticated account of criminal responsibility is informed by appreciation of criminal law as a complex social institution.³⁸ On Lacey's account, criminal responsibility cannot be theorised without detailed scrutiny of 'existing social practice[s]' informed by socio-historical drivers to criminalisation.³⁹

Sharing this intellectual lineage, central to Farmer's account is the criminal law as an institution which operates to secure civil order.⁴⁰ Civil order is not a fixed idea but involves coordination of 'individuals and their interests'.⁴¹ Criminal law works to secure coordination of those interests, 'establishing measures for building and reinforcing trust between individuals'.⁴² Farmer's provocation for criminal law theorists is to investigate how the criminal law as an institution has been used 'to secure civil order and build civil society and understandings of citizenship'.⁴³ On Farmer's account, criminalisation is not a discrete and independent area of study but is embedded within 'fundamental questions about the nature of social and civil order and the role of government and the state in building that order'.⁴⁴

Lacey and Farmer's accounts both highlight the importance of scrutinising the ways in which the criminal law has been shaped by interests and power structures over time, including underlying ideas which have informed the scope and limits of the criminal law. To this we can add a further prism for analysis which is highly relevant to this paper's conceptual work on fraud. Farmer has argued that the institution of criminal law is in symbiotic relationship with the market, which is 'central to how we think of civil order'.⁴⁵ Herzog's definition of the market is used as places of exchange of goods and services, often supported by 'money as a medium of exchange', enabling the setting of prices.⁴⁶ On Farmer's

³⁴Holder, above n 15, pp 455–457.

³⁵Ibid, p 422.

³⁶L Farmer 'The "market" in criminal law theory' (2022) 85(2) *Modern Law Review* 435 at 456.

³⁷Farmer, above n 12, p 117.

³⁸Lacey, above n 12.

³⁹Ibid, p 185.

⁴⁰Farmer, above n 12, p 117.

⁴¹Ibid, p 117.

⁴²Ibid, p 299.

⁴³Ibid, p 117.

⁴⁴Ibid, p 117. And N Lacey 'Approaching or rethinking the terrain of criminal law?' (2020) 14 *Criminal Law and Philosophy* 307.

⁴⁵Farmer, above n 36, p 458.

⁴⁶L Herzog 'Markets' in EN Zalta (ed) *The Stanford Encyclopedia of Philosophy* (Fall 2017 edn) <https://plato.stanford.edu/archives/fall2017/entries/markets/>.

account, markets are intrinsically tied not only to exchange of goods and services but also to civil order in that they involve the coordination of individuals ‘in increasingly socially complex societies’.⁴⁷ A key insight is that:

... certain kinds of wrongdoing (‘control’ frauds, insider dealing, money laundering etc.) are generated by markets themselves, and so in thinking about these crimes there is little prospect of access to ‘natural’ moral categories to understand or classify conduct. The moral understandings of the wrongdoing depend on and are shaped by changing understandings of permissible conduct in that market situation.⁴⁸

Taking Farmer’s market-based analysis further, there is a key and unexplored relationship between fraud and the market. The starting position, for reasons I explain in the second section below, must now be that fraud is a dominant form of contemporary market conduct. Fraud is embedded within contemporary markets, *feeding into and shaping* the civil and political institution of the criminal law. With some irony, fraud is part of the institutional set-up of civil order which the criminal law seeks to secure. This means that analysis of fraud’s meanings in its dominant context is central to understanding fraud. Contextualising the trajectory of fraud within its dominant context allows us to have a more nuanced understanding of a wrong which the criminal law seeks to address. It also enables us to better understand fraud’s pervasive role in society *and* within the institution of the criminal law.

Contextualising fraud as a dominant form of contemporary market conduct also acknowledges the prevalence and use of the term ‘scam’ in public discourse and media, as a related form of market conduct.⁴⁹ Mark Button and Cassandra Cross have argued that scams can be distinguished as a less culpable form of conduct than fraud, the former relying on deceptive persuasion and emotional manipulation involving direct engagement with victims.⁵⁰ ‘Scams’ may shift blame onto victims by labelling them as gullible rather than having been deceived.⁵¹ The industrialisation of fraud suggests no clear lines between scam and frauds but embeds both as dominant forms of market conduct in the digitalised economy. As the most serious form of market conduct linked to criminal liability, analysis of fraud is given prominence in this paper.

2. The industrialisation of fraud

The focus of this section is to think about fraud’s core norms in a distinctive way, by interrogating their scope within their surrounding dominant context. I argue that the digitalised economy is now the key context for unpacking fraud. This is because there has been a significant shift in fraud, both in the real world and conceptually. In the real world, fraud is now fully embedded within a cross-border, thriving, global digitalised economy.⁵² The digitalised economy is not an essential context or ‘add on’ to fraud. It provides more than opportunities for fraud or a marketplace for fraud to grow, replicate and evolve. Rather, evolution in design and implementation of fraud is now shaped and propelled by the digitalised economy.

An illustrative example can be found in the case of *R v Steven Cooper, David Park, Tejay Fletcher*.⁵³ This was a combined appeal in which the Court of Appeal was tasked with considering the approach to

⁴⁷Farmer, above n 36, at 451.

⁴⁸*Ibid.*, at 459.

⁴⁹Home Office *Stop! Think Fraud* (12 February 2024) <https://www.gov.uk/government/news/major-campaign-to-fight-fraud-launched>.

⁵⁰M Button and C Cross *Cyber Frauds, Scams and their Victims* (London: Routledge, 2017) pp 6–8.

⁵¹AARP and FINRA Investor Education Foundation *Blame and Shame in the Context of Financial Fraud* (2022).

⁵²R Hyde and JA Gibson ‘Fraudscape: the size of the fraud problem around the world’ (London: Social Market Foundation, 2024).

⁵³*R v Steven Cooper, David Park, Tejay Fletcher* [2023] EWCA Crim 945.

totality in sentencing undertaken in relation to the Proceeds of Crime Act 2002. The appellant had been responsible for software called ‘iSpooF’, for which subscribers paid for access. They were able to use tools provided by this software to commit fraud. Together, these tools included voice manipulation software, the ability to intercept passwords and other personal data, as well as control over call diversions. This was complemented by a suite of explanatory videos for users.⁵⁴ These tools were used to facilitate widescale impersonation of banks by individuals on a global scale.⁵⁵ It was estimated at trial that frauds conducted using iSpooF in the UK exceeded £43 million.⁵⁶ Global losses were estimated at £100 million.⁵⁷ In one example an individual’s losses ran to £2 million, having believed the false representation that their contact was a bank employee.⁵⁸

In considering the appeal on the totality of sentences applied in the *Fletcher* case, the Court of Appeal noted the scale of the persons targeted being ‘very much higher than can ever be the case using more traditional methods of fraud’.⁵⁹ The Court emphasised the hidden nature of such a large fraudulent network, propelled via software systems, increasing the vulnerability of the general population to fraud. It also noted how iSpooF technology undermined public trust in conducting financial transactions, thus requiring ever more complex verification systems for transactions. The implications for sentencing are significant: ‘The power of the Internet to enable fraud on a massive scale is a factor which must be considered’.⁶⁰ According to the Court, the prospect for future technological developments in creating new methods for misleading people or sending out fake communications increases this threat.⁶¹

The pace and scale of real-world changes in fraud is significant. *R v Steven Cooper* provides one stark illustration of this point. Other examples could be given.⁶² It is the conceptual shift – characterised here as the ‘industrialisation’ of fraud – which is critical for the analysis that follows. This conceptual shift provides the foundation for placing the digitalised economy at the heart of unpacking fraud. The industrialisation of fraud is underpinned by the global digitalised economy. Fraud is industrialised because of this economy. Taking this argument further, the digital economy grows and thrives with fraud as part of its (unregulated) core, operating at scale, across borders and with technological innovations as its driver. Fraud is operationalised and subject to change within this context and its meanings must be unpacked within this setting. It follows that an account of fraud’s meanings without the digitalised economy is fundamentally incomplete. To date there has not been scrutiny of this relationship in criminal law literature on fraud.

To secure this foundational argument for putting the digitalised economy at the heart of theorising fraud, the following questions require attention: (i) what is meant by the digitalised economy? Is this a coherent, stable and distinctive idea? Next, (ii) can we explain and justify the industrialisation of fraud?

(a) The digitalised economy

We turn first to what is meant by the digitalised economy. Don Tapscott adopted the narrower term ‘digital economy’ in 1996 in *The Digital Economy: Promise and Peril in The Age of Networked Intelligence*.⁶³ While not explicitly defining the term, Tapscott argued that the digital economy is

⁵⁴Ibid, at [43].

⁵⁵Between September 2021 and August 2022, 10 million fraudulent calls were made globally, with circa 3.5 million in the UK: see *Fraud Strategy*, above n 5, p 19.

⁵⁶Above n 53, at [44].

⁵⁷Ibid, at [44].

⁵⁸Ibid, at [49].

⁵⁹Ibid, at [61].

⁶⁰Ibid, at [61].

⁶¹Ibid, at [61].

⁶²‘INTERPOL financial fraud assessment: a global threat boosted by technology’ (22 March 2024) <https://www.interpol.int/en/News-and-Events/News/2024/INTERPOL-Financial-Fraud-assessment-A-global-threat-boosted-by-technology>.

⁶³D Tapscott *The Digital Economy: Promise and Peril in the Age of Networked Intelligence* (New York: McGraw-Hill Education, 1996).

illuminated by a series of emerging relationships between people, business, government and technology, and how these relationships co-depend on each other.⁶⁴ Tapscott's framing of human networking, achieved through technology, has been identified as part of a fourth industrial revolution. While the contours of a fourth industrial revolution are heavily contested, major technology innovations built on earlier industrial revolutions.⁶⁵ The first industrial revolution in the mid-18th century to early 19th century was prompted by developments in transport infrastructure, including canal networks and preliminary railway tracks.⁶⁶ This was supported by early innovations in machinery developments, such as through invention of the Spinning Jenny and low-pressure steam engines.⁶⁷ A second revolution, which began in 1870, made further progress, propelling a move from home-spinning and small-scale production to large-scale factory outputs, allowing for goods to be transported more widely.⁶⁸ Economies of scale became possible.⁶⁹ A third industrial revolution (circa 1950s) was shaped by rapid changes in communication systems, via new accessibility to personal computers, followed by the invention of the Internet.⁷⁰

Work on the digital economy and its conceptual parameters has progressed rapidly from Tapscott's early framing. In the 2000s and 2010s the focus was on how information and communication technologies were influencing economic change.⁷¹ Of interest were electronic means of production which enabled trade of 'goods and services through electronic commerce on the Internet'.⁷² Examples included closer connections between sellers or service providers and their end-users, facilitated through increasing ownership and use of personal computers, laptops, mobile phones and, eventually, smart-phones. Complementing this was the increasing dominance of online digital platforms to provide goods and services. A further key aspect at this time was the centralisation of data and increasingly its uses in algorithmic decision-making and analytics.⁷³

Conceptual work into the digital economy has since recognised that framing of the digital economy to include direct applications of Information Technologies and Information Communication Technologies is a narrow view. In their seminal paper on the topic, Rumana Bukht and Richard Heeks note that this places telecommunications, software, hardware manufacture and information services at the core of a conceptual account.⁷⁴ A more expansive view focuses on a core digital sector.⁷⁵ This model presents the digital economy as 'part of economic output derived solely or primarily from digital technologies with a business model based on digital goods or services'.⁷⁶ In this framing, there is scope to consider sharing and gig economies.⁷⁷

⁶⁴Ibid, p 12.

⁶⁵A Anyimadu et al 'Experimentalism and the fourth industrial revolution' (London: Open Data Institute, 2022).

⁶⁶R Allen *The British Industrial Revolution in Global Perspective* (Cambridge: Cambridge University Press, 2014) pp 273–275.

⁶⁷J Styles 'The rise and fall of the Spinning Jenny: domestic mechanisation in eighteenth-century cotton spinning' (2020) 51(2) *Textile History* 195; J Farey *A Treatise on the Steam Engine: Historical, Practical and Descriptive*, 1827 (Newton Abbot: David & Charles Reprints, 1971).

⁶⁸See J Mokyr *The Lever of Riches: Technological Creativity and Economic Progress* (Oxford: Oxford University Press, 1992).

⁶⁹See Anyimadu et al, above n 65.

⁷⁰J Rifkin *The Third Industrial Revolution: How Lateral Power is Transforming Energy, the Economy, and the World* (London: Palgrave Macmillan, 2011).

⁷¹R Bukht and R Heeks 'Defining, conceptualising and measuring the digital economy' (Development Informatics Working Paper No 68, 2017) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3431732.

⁷²OECD *The Digital Economy* (OECD Paris, No 151, 2012) p 5.

⁷³Bukht and Heeks, above n 71, p 12.

⁷⁴Ibid, p 13. It is not the purpose of this paper to map current developments onto a clear stage of industrial revolution. See M Knell 'The digital revolution and digitalised network society' (2021) 2 *Review of Evolutionary Political Economy* 9; UN Policy Brief: *Digital Economic Transformation* https://www.un.org/sites/un2.un.org/files/digital_economy_14_march.pdf.

⁷⁵Bukht and Heeks, above n 71, p 13, characterised by Bukht and Heeks as the digital economy of narrow scope.

⁷⁶Ibid, p 13.

⁷⁷Ibid, p 13.

It is the broadest framing – the digitalised economy – which is most compelling for this paper’s study of fraud. On this model, e-business, e-commerce, industry, precision agriculture, algorithmic economy and the sharing and gig economies are brought into conceptual view.⁷⁸ Within this framing of a digitalised economy, ‘disruptive technologies’, with wide-ranging spheres of influence, are placed front and forward.⁷⁹ These technologies cluster around four animating ideas. The first relates to hyperconnectivity, meaning the ‘growing interconnectedness of people, organisations, and machines that results from the Internet, mobile technology and the internet of things (IoT)’.⁸⁰ A second relates to increasing sophistication in analytics and intelligence. A third relates to human machine interaction, including by automation or semi-automation.⁸¹ Finally, a fourth acknowledges that technological disruptions of the digitalised economy are underpinned by advanced engineering.⁸² The importance of data is embedded throughout production processes of the digitalised economy.⁸³ I home in on other features of the digitalised economy in identifying fraud’s footholds, below.

Incorporating a model of the digitalised economy into industrialised fraud provides the strongest basis for interrogating knowledge flows within global networked economies. It allows for interrogation of digital technologies, digital infrastructure, digital services and data with a particular interest in emerging forms of transactional practices. These may be facilitated by emerging technologies. This is of interest for this study of fraud’s meanings as we know that emerging ways of transacting entice fraudsters. Conceptual work on fraud requires underpinning within a global networked economy, questioning how fraud sits within, and is shaped by, widespread digitalisation of the economy and society.

(b) The industrialisation of fraud within the digitalised economy

The key conceptual shift, I argue, is the industrialisation of fraud, underpinned by the digitalised economy. The relationship between fraud and the digitalised economy is symbiotic. It is this conceptual shift which provides the foundation for placing the digitalised economy at the heart of unpacking fraud. Can we explain and justify the industrialisation of fraud?

I understand ‘industrialisation’ of fraud as meaning social, structural, technological, and economic transformations of the digitalised economy which embed fraud at scale and across borders. These transformations occur within the businesses and practices of the digitalised economy *and* within its interpersonal interactions.⁸⁴ It pushes beyond interpersonal relationships as central cases of fraud, whilst not denying that these remain key to industrialised fraud. The focus of this theoretical framing of fraud is upon fraud’s core norms, operating within the structural building blocks provided by the digitalised economy. These building blocks allow fraud to thrive, grow and evolve. Technological revolution is at the heart of the industrialisation of fraud.

The industrialisation of fraud also relates to fraud’s placement within a modern economy and society. Industrialised fraud is spurred along by the digitalised economy, but it is also embedded within it. Fraud is industrialised within and because of this economy. Industrialised fraud is another way of conceptualising a ‘global scam economy’.⁸⁵ In this framing, fraud is no longer the outlier but is part of unregulated business as usual. It is therefore irrelevant whether fraudulent interactions have an explicit digital

⁷⁸Ibid, p 13.

⁷⁹J Manyika et al ‘Disruptive technologies: advances that will transform life, business, and the global economy’ (New York: McKinsey Global Institute, 2013).

⁸⁰Deloitte ‘What is digital economy’ (New York: Deloitte, 2017) <https://www2.deloitte.com/mt/en/pages/technology/articles/mt-what-is-digital-economy.html>.

⁸¹Resulting in changes to worker-upskilling and system-management: see Knell, above n 74, at 15–21.

⁸²R Heeks *Information and Communication Technology for Development* (Abingdon: Routledge, 2017).

⁸³M Mueller and K Grindal ‘Data flows and the digital economy: information as a mobile factor of production’ (2019) 21(1) Digital Policy, Regulation and Governance 71.

⁸⁴*Fraud Strategy*, above n 5, pp 7–12.

⁸⁵K Tedder ‘The escalation of digital fraud: global impact of the coronavirus’ (October 2020) https://javelinstrategy.com/sites/default/files/files/reports/20-5010J-FM-The%20Escalation%20of%20Digital%20Fraud-SAS_0.pdf.

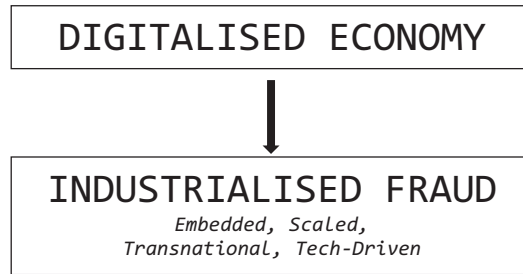


Figure 1. Fraud in the Digitalised Economy.

dimension or overt connection to the digitalised economy. The argument is that fraudulent practices are so embedded within the digitalised economy that they must be considered as part of it. This extends to considering those who ignore or permit fraud (for example, on online platforms for which they are responsible), as well as those who are actively involved in assisting or encouraging fraud and scams online and in interpersonal relationships.

The conceptual shift whereby fraud is now situated within a digitalised economy – the industrialisation of fraud – requires that the digitalised economy be at the heart of unpacking fraud’s meanings. Criminal law literature on fraud must now interrogate fraud’s meanings *within* the context of the digitalised economy. This point is represented in Figure 1.

(c) *Fraud’s footholds*

This sub-section examines a set of structural footholds provided by the digitalised economy which shape fraud’s meanings. By footholds I mean ‘a strong or favourable position from which further advances or progress may be made’.⁸⁶ As a climber uses footholds to scale a climbing wall, fraud thrives, multiplies and evolves through using footholds embedded in the digitalised economy. Seven (non-exhaustive) illustrative examples of relevant footholds can be identified.

It must be emphasised that fraud’s footholds amount to more than (new) opportunities for fraud.⁸⁷ It is unremarkable that fraudsters will take advantage of contextual changes, using these as opportunities for fraud. Recent examples include the cost-of-living crisis prompting scams around promising cheaper utilities bills.⁸⁸ Previously the Covid-19 pandemic led to an increase in fraud related to online shopping because of the dominance of online transactions at that time.⁸⁹ Fraud’s footholds are important because they are actively influencing the contours of fraud’s norms in a digital age. They exert stronger influence than simply providing opportunities for fraud.

A first foothold for fraud is provided by digital hyperconnectivity being a key feature of the digitalised economy. Rogers Brubaker identifies this as ‘the condition in which everyone is (potentially) connected to everyone, to an exponentially growing array of sensor-embedded things, and to an infinity of digital content, everywhere and all the time’.⁹⁰ An inter-connected world has influenced and shaped many parts of society, including norms and expectations of social interaction, relationships and self. Examples

⁸⁶Collins English Dictionary ‘foothold’ <https://www.collinsdictionary.com/dictionary/english/foothold>.

⁸⁷D Cressey ‘Why do trusted persons commit fraud? A social-psychological study of defalcators’ (1951) *Journal of Accountancy* 576.

⁸⁸F Lipson ‘Seven energy scams to watch out for’ (Which?, 2022) <https://www.which.co.uk/news/article/7-energy-scams-to-watch-out-for-a7hWE2O98VCm>. For pre-fourth industrial revolution, see E Balleisen *Fraud: An American History from Barnum to Madoff* (Princeton: Princeton University Press, 2018).

⁸⁹Statista *Impact of the Covid-19 Pandemic on Fraud Attempts and Fraud Rate According to Online Merchants Worldwide in 2021* (Hamburg: Statista, 2024).

⁹⁰R Brubaker ‘Digital hyperconnectivity and the self’ (2020) 49 *Theory and Society* 771; R Brubaker *Hyperconnectivity and Its Discontents* (Cambridge: Polity Press, 2022).

include the presence of instant messaging, online marketplaces and multi-layered levels of connectivity between persons and businesses.

Secondly, and linked to hyperconnectivity, is a foothold of accessibility. Accessibility, facilitated by online technologies, is a key feature of the digitalised economy. It means that flows of information capital are not constrained by physical borders but operate smoothly on a global scale with low barriers to entry.⁹¹ Accessibility will not always be equitably distributed or inclusive, as it depends upon a population being Internet-connected. There may be an uneven distribution of accessibility across the Global North and Global South, for example.⁹² Both digital hyperconnectivity and online accessibility lead to fraud's inherent transnational operation.

A third foothold for fraud arises from the centrality of data – especially consumer data – to the digitalised economy. The OECD identifies drivers towards 'Big Data' as linked to 'the increasing migration of socio-economic activities to the Internet', as well as declines 'in the cost of data collection, storage and processing'.⁹³ Doug Laney ties 'Big Data' to the volume of data involved, data's transmission in real-time, and variety data forms.⁹⁴ 'Big Data' provides a global data marketplace, monetised through access gateways to data, as well as through storage of personal data.⁹⁵

A fourth foothold arises from rapid content creation (including by automation and semi-automation) and consumption. Innovative technologies, such as generative artificial intelligence, have an influential role in supporting this. By automating self-learning, platforms like ChatGPT and CoPilot allow individuals to access contextualised knowledge quickly.⁹⁶ They also provide a sophisticated and far-reaching tool to conduct realistic impersonation or phishing at high volume. They can reproduce language patterns to allow for impersonation of a particular speech style or technique with a high degree of accuracy.⁹⁷

Bolstered by emerging technologies involving algorithmic targeting and behavioural analytics, a fifth foothold is provided by personalisation. Distinct from customisation, personalisation involves tailoring a good or service towards a particular individual or individuals' needs.⁹⁸ An industry around personalisation has sprung up within the digitalised economy.⁹⁹ Personalisation lays the groundwork for trust, given that an interaction, service, good or payment appears directed at a particular person, even if it has been sent out *en masse*. For example, a representation made over instant messaging could be amended, via automation, to include personalisation. Personal communication, which appears tailored to an individual's circumstances or preferences, lays the basis for manipulating another person into authorising a fraudulent transaction.

A sixth foothold for fraud is the significance of e-commerce and e-business, animated by the promise of faster payments as the model of business as usual.¹⁰⁰ Many personal and business transactions now occur online and at speed. Transaction speed is enhanced by growth in cryptocurrency, which enables fast transnational transactions without the need for a regulated intermediary, such as a bank. For

⁹¹M Leese et al 'Data matters: the politics and practices of digital border and migration management' (2022) 27(1) *Geopolitics* 5.

⁹²See B Kilic and R Avila 'Cross border data flows, privacy and global inequality' (Public Citizen) <https://www.citizen.org/wp-content/uploads/crossborder-data-flows-privacy.pdf>.

⁹³OECD *Data-Driven Innovation: Big Data for Growth and Well-Being* (Paris: OECD Publishing, 2015) p 4.

⁹⁴D Laney '3D data management: controlling data volume, velocity and variety' (META Group Research Note, 2001) p 6.

⁹⁵*Ibid*, p 6.

⁹⁶See Europol, above n 6, for discussion of ChatGPT.

⁹⁷K Hu 'ChatGPT sets record for fastest-growing user base – analyst note' (Thomson Reuters, 2023) <https://www.reuters.com/technology/chatgpt-sets-record-fastest-growing-user-base-analyst-note-2023-02-01/>.

⁹⁸Oxford English Dictionary 'personalisation' <https://www.oed.com/search/dictionary/?scope=Entries&q=personalisation&tl=true>.

⁹⁹T Nisar *Personalization and Digital Social Markets: Disrupting the Capitalist Economy* (London: Bloomsbury Publishing, 2025).

¹⁰⁰Bank for International Settlements *Fast Payments – Enhancing the Speed and Availability of Retail Payment* (Basel: BIS, 2016).

example, Coinbase is a cryptocurrency which is underpinned and secured by Blockchain technology.¹⁰¹ Crucially, these transactions are not reversible. Cryptocurrency transactions therefore allow for fraud to occur quickly and for proceeds to be irreversibly channelled away.

Finally, fragmented accountability and governance structures of the digitalised economy, and its surrounding regulatory environment, provide a foothold for fraud. Just as a robust regulatory environment underpins the health of a global digitalised economy, contributing to trust and transparency, so too voluntary and mandatory regulation of Big Tech and online platforms may lead to structures which incentivise or disincentivise fraud.¹⁰² Significant is the recent implementation of mandatory reimbursement for victims of authorised push payment fraud in England and Wales up to a maximum of £85,000.¹⁰³ While this might appear to be a response to fraud, it is also a foothold for fraud in the digitalised economy. This is because it changes risk appetite around fraud. If individuals know that they will be reimbursed by their bank if it turns out that the transaction they authorised was fraudulent, there may be an increase in the number of people willing to run the risk of fraud. Cross-border organisational structures within the digitalised economy are critically important and will promote or suppress internal or external fraud, as well as inform where fraudsters choose to perpetrate fraud, dependent on enforcement structures.¹⁰⁴ Cassandra Cross has powerfully explained how perpetrators of fraud exploit jurisdiction to ensure that they cannot be pursued by law enforcement.¹⁰⁵

The argument can be represented visually as follows in Figure 2:

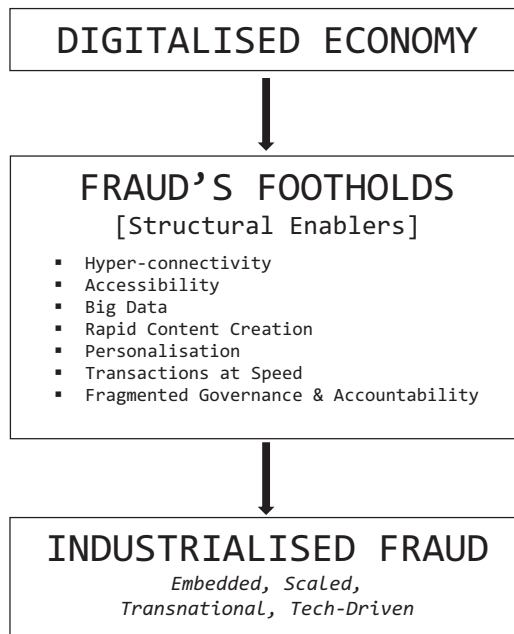


Figure 2. Fraud's Footholds.

¹⁰¹See <https://www.wearepay.uk/what-we-do/payment-systems/faster-payment-system/>.

¹⁰²Department for Digital, Culture, Media and Sport and Department for Business, Energy and Industrial Strategy *A New Pro-Competition Regime for Digital Markets* CP 657 (HMSO, 2021).

¹⁰³Financial Services and Markets Act 2023, s 72.

¹⁰⁴National Audit Office 'Tackling fraud and corruption against government' HC 1199 (2022–23) <https://www.nao.org.uk/press-releases/tackling-fraud-and-corruption-against-government/>.

¹⁰⁵C Cross "'Oh we can't actually do anything about that': the problematic nature of jurisdiction for online fraud victims' (2020) 20(3) *Criminology & Criminal Justice* 362.

3. Industrialised fraud: understanding fraud in a digital era

I argue that the digitalised economy provides more than just essential context for unpacking fraud’s meanings. More radically, fraud’s core norms are being reshaped by structural aspects of the digitalised economy. Examination of fraud’s footholds within a digitalised economy sheds new and unexplored light on fraud’s meanings for those interested in the criminal law’s response to fraud. I reappraise fraud’s core norms through analysis of fraud’s means, purposes and fault.

Alongside this I introduce a further lens for conceptual analysis – consideration of fraud’s lifecycles, to involve an approach stage, interaction and/or an outbound stage. This is because fraud has complex temporal dimensions in the digitalised economy.¹⁰⁶ Industrialised fraud – the transformation which has occurred within the business and practices of the digitalised economy and within its interpersonal interactions – has created cyclical patterns by which fraud evolves, thrives and multiplies. In the digitalised economy, fraud’s design and implementation influences the contours of fraud. There will be various levels of sophistication in planning and targeting victims, including organised and spontaneous. It also considers how and when the gains of fraud are channelled away within a conceptual account of fraud. The aim of integrating analysis of fraud’s lifecycles is to break down further *how* fraud’s footholds are being used in the digitalised economy, thereby shedding fresh light on the contours of fraud. The following visual in Figure 3 encapsulates the relevance of fraud’s lifecycles:

(a) *Fraud’s means*

A first set of argument explores how fraud’s footholds are reframing the contours of fraud’s core means. As explored in Section 1 above, criminal law literature on fraud has focused on fraud as trickery used to gain a dishonest advantage (often financial) over another person. This has also been identified as an act of dishonesty. Another prism for thinking about fraud’s means is through the conduct outlined in sections 2–4 of the Fraud Act 2006, as involving deliberate false representation, failure to disclose information or abuse of a position of trust. Fraud’s means connect to all the footholds outlined in Section 2(c) above. For the purposes of this paper, highly significant are footholds of rapid content creation (including by automation or partial automation) and consumption, and the role of innovative technologies, such as generative artificial intelligence in supporting this. Also relevant is the dominance of e-commerce and e-business, alongside the further foothold of personalisation.

How can fraud’s core means be reframed within the digitalised economy? Fraud’s footholds – which provide the key infrastructure and capability for fraud – represent that the digitalised economy is embedded in all cases of fraud to a greater or lesser extent, not just those which overtly use technology. Fraudulent conduct is foundationally connected to the online environment, supported by innovative technologies. Moreover, a focus on fraud’s footholds supports an argument that there is greater range and variety to fraud’s means within the digitalised economy, signifying new forms and methods to

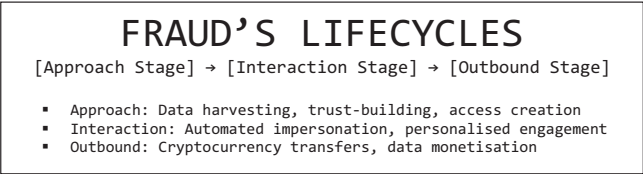


Figure 3. Fraud’s Lifecycles.

¹⁰⁶There are similarities with the House of Lords *Fighting Fraud: Breaking the Chain*, above n 5, p 23, which identifies a ‘fraud chain’. I adopt the language of lifecycle/s. This acknowledges that there may be no approach stage by which to formulate a ‘fraud chain’. Moreover, the endpoint of fraud may be difficult to identify (knowledge gains rather than financial gains) in a digital ecosystem.

fraudulent innovation. A robust conceptual account of fraud's meanings must highlight digitalisation of fraud's means *within* a core account of fraud's meanings. Fraud's means are being reshaped around content creation using automated forms and personalisation. This may be supported by emerging technologies, such as generative AI in creating relevant content/misrepresentations and automated fraud. Platforms like ChatGPT can draft highly authentic texts which may have been previously detectable as fraudulent due to poor spelling and/or grammar.¹⁰⁷ The effect is to enable fraud which can be created faster, more authentically and at increased scale and reach.

This means that accounts of fraud for those interested in criminal law must now move beyond general references to deceit or the making of false representations. Fraud's new forms and methods ought to be explicitly acknowledged. This could be achieved through descriptors of AI-enabled fraud; AI-generated fraud; AI-dependent fraud and AI-targeted fraud in unpacking fraud.¹⁰⁸ It is a separate question what relevance fraud's methods have to criminalisation and to sentencing. This also requires embedding *prospects* for fraud innovation in the digitalised economy within core normative accounts of fraud's meanings. Hypothesising about the next decade for fraud, new *modi operandi* for fraud are to be expected which are AI-generated. There have been recent efficiencies in the AI which underpin deepfakes, for example.¹⁰⁹ Not only can mouthparts now move; they can also change and adapt the video content to deliver in a different language and with the mouthparts moving accordingly. This allows for operation across jurisdictions in different languages. Improvements around greater authenticity and accuracy means that generated messages or representations have a higher prospect of resonating with their recipient.¹¹⁰

(i) *Fraud's lifecycles: inbound routes*

We can further unpack fraud's means by focusing on inbound routes to fraud. This can also be identified as fraud's approach stage. The laying of groundwork for fraud is a distinctive aspect of fraud which must take on conceptual prominence in the digital era. An inbound route or approach stage relates to implementation of measures to establish key information or connections for dishonestly gaining an advantage over another person. This could be achieved by putting pressure upon a targeted individual or by engaging in surveillance tactics. These are measures, implemented deliberately, which *pave the way* for fraud. The methods of approach which are of interest ought to have causal significance to the fraud itself (i.e. they cannot be so far removed as to be irrelevant).

A wide range of causally significant phenomena may come within an approach stage, embedded within the digitalised economy. They give further explanation as to how fraud's footholds are used to perpetrate fraud. Within the digitalised economy it is to be expected that the approach stage to fraud will be facilitated by digital means. For example, mass 'phishing' exercises can be assisted by automated means such as SIM farms which allow for text messages to be sent out at scale.¹¹¹

The conceptual model which should now be prioritised in understanding fraud is that fraud's footholds are not always used in a one-off transaction. The use of fraud's footholds can, in the first instance, be used to create and/or support an approach stage for fraud. Depending on whether fraud is organised or spontaneous, distinct levels of sophistication in planning and implementation may be present. Relevant measures include steps taken to build interpersonal trust, through friendship or by appearing to offer help in a crisis. This aligns an account of fraud's meanings with how fraud is operating

¹⁰⁷Europol, above n 6, p 7.

¹⁰⁸M Caldwell et al 'AI-enabled future crime' (2020) 9 Crime Science 14. On generative AI, see A Janjeva et al 'The rapid rise of generative AI: assessing risks to safety and security' (London: The Alan Turing Institute, 2023).

¹⁰⁹N Schick *Deepfakes: The Coming of Infocalypse* (London: Monoray, 2020).

¹¹⁰NC Köbis et al 'Fooled twice: people cannot detect deepfakes but think they can' (2021) 24(11) iScience 103364. Representations feel normalised in that there are no spelling or grammar mistakes to 'flag' for the receiver that an interaction may be fraudulent.

¹¹¹*Fighting Fraud*, above n 5, at [64]: 'Phishing is the practice of sending fraudulent communication that appears to come from a reputable source. Smishing is the same practice but refers to the use of SMS text messages to defraud victims'.

in the real world. For example, authorised push payment (APP) fraud involves persuading an individual to act quickly. A common example relates to impersonating a representative from a targeted individual's bank, persuading them to make an urgent payment to a false account. The aim is to lay a robust pathway for fraud. An alternative causally relevant approach stage to fraud may involve creating access route/s to information necessary for fraud. Examples of this would include harvesting data and personal information, achieved through phishing expeditions. It could also include gaining remote access to devices, providing gateways to personal information.¹¹² Focus on an approach stage to fraud within the digital economy places importance on causally significant pathways to fraud. It gives credence to the idea of 'fraud staging' within a conceptual account of fraud's meanings.¹¹³

(ii) *Fraud's lifecycles: interaction*

The second point of interest in unpacking fraud's means comes from considering fraud's interaction stage. Classic process accounts of fraud exclude this element from view. For example, fraud by a false representation does not directly focus on whether a false representation has been received by another person. Fraud facilitated by abuse of a position of trust challenges this approach to some extent. It is compelling that we would want to question background contextual issues prior to determining whether there has been abuse of a relevant position of trust for the purposes of fraud by abuse of position.¹¹⁴

Expansion of the digitalised economy and its footholds of rapid content creation (including by automation) and consumption, the dominant roles of innovative technologies, of e-commerce and e-business, alongside personalisation, provide a fertile ground for fraud. Fraud can be sent out (by automation, another entity or by a person) indiscriminately by individuals, groups of individuals, or bots to see who 'bites'.¹¹⁵ Digital methodologies provide a means for fraud to be reproduced rapidly. In these ways part of fraud's new conceptual framing must emphasise that an interaction stage may *not* be present in core cases of fraud. A focus on fraud's interaction stage highlights a complexity at the heart of industrialised fraud. Industrialised fraud can achieve highly personalised fraud, *en masse*, without the need for interpersonal interactions. This will often be facilitated by emerging technologies.¹¹⁶ These play upon a universal type of vulnerability for individuals who are transacting and socialising in the digitalised economy.¹¹⁷ In a digitalised economy there is no necessary sense in which fraud must be interpersonal or have an element of interaction with its intended targets.

There is further complexity to fraud's interaction stage within the digitalised economy. Concurrently, interpersonal, highly personalised and interactive means are *also* key ways in which fraud's footholds are used. In some cases, interaction between a fraudster and their targeted individual will be front and forward. This is not necessarily limited to small-scale interpersonal interactions. For example, it is possible for fraud at scale to be highly personal in how it grafts the target of fraud into a scheme. Industrialised fraud allows representations to be sent at scale to see who bites.¹¹⁸ In an era characterised by hyperconnectivity, many individuals can be reached by one false representation at one time. It can then directly graft (through communication) the target of fraud into a relationship premised on trickery, to ensure that money is transferred to a fraudster.¹¹⁹ This leads to a wider net of fraud victims, as evidenced by the iSpoof model.¹²⁰

¹¹²*Fraud Strategy*, above n 5, p 11.

¹¹³*Fighting Fraud*, above n 5, ch 2.

¹¹⁴J Collins 'Fraud by abuse of position and unlicensed gangmasters' (2016) 79(2) *Modern Law Review* 354.

¹¹⁵*Fraud Strategy*, above n 5, p 11.

¹¹⁶For example, by account takeover.

¹¹⁷N Helberger et al 'Choice architectures in the digital economy: towards a new understanding of digital vulnerability' (2022) 45 *Journal of Consumer Policy* 175.

¹¹⁸LabHost, an online platform, enabled impersonation of over 170 trusted organisations: see Metropolitan Police 'Law enforcement infiltrates fraud platform used by thousands of criminals worldwide' (Press Release, 2024) <https://www.europol.europa.eu/media-press/newsroom/news/international-investigation-disrupts-phishing-service-platform-labhost>.

¹¹⁹For example, APP fraud.

¹²⁰*Fighting Fraud*, above n 5, p 5.

Fraud's potential for interpersonal interaction with its victims in a digitalised economy requires exploration. This gives scope to bring vulnerability within the conceptual analysis of fraud. Vulnerability should be understood broadly, using Martha Fineman's account of 'the primal human condition'.¹²¹ On this account, vulnerability characterises individuals regardless of intelligence, race, class, wealth, and social standing. This is the version of vulnerability which is most compelling in developing fraud law scholarship. The 'universality and constancy of vulnerability' put forward by Fineman is particularly relevant to the study of fraud's meanings.¹²² While some groups may be more prone to fall victim to fraud, there is a form of vulnerability to fraud for all individuals who are interacting, transacting and socialising in a digitalised society.¹²³ Both inbound and interaction elements of fraud's lifecycles may involve engagement with vulnerability. Fraud is quite different from other offences of dishonesty, such as theft or burglary, which do not have this involvement from victims at the core of central cases. The most similar example may be found in the context of grooming for sexual offences.¹²⁴ Grafting the target of fraud into fraud does not involve blaming victims or claiming that they are responsible for this wrongdoing. Rather, a conceptual account of fraud's meanings must give credence to the powerful way in which fraudsters can operate industrially, in a personalised way, to perpetrate fraud.

(b) Fraud's purposes

Fraud's footholds in the digitalised economy also reshape our understanding of fraud's purposes. There is some irony in making this argument, as current framings of fraud's purposes in England and Wales are set broadly. Section 1 above unpacked how current criminal law literature on fraud has focused upon an intention to gain an advantage over another person. This has been elaborated legally in the Fraud Act 2006 as requiring intention to gain or to cause loss or the risk of loss, often financially, over another person. The parameters of what amounts to 'gain' or 'loss' have been set broadly. Section 5 of the Fraud Act 2006 identifies 'gain' and 'loss' as covering 'gain or loss in money or property (meaning whether real or personal, including things in action and other intangible property)'.

A focus on fraud's footholds, provided by the digitalised economy, gives a richer basis for explaining how the digital age is powerfully reshaping fraud's purposes. Fraud's purposes are now shaped by footholds of data availability and accessibility, as well as the foothold of hyperconnectivity.¹²⁵ These are complemented by two further footholds – the online sphere being the dominant sphere for transactions and the development of interpersonal relationships, and the foothold for fraud provided by personalisation.

Together these footholds point to the central placement of data and information capital within the production processes of the digitalised economy. The digitalised economy provides a conceptual foundation for fraud's purposes which is data-driven and information-rich. Linked to this, data surveillance is highly relevant in supporting a highly networked world.¹²⁶ Information advantage is now a key commodity. Danielle Citron notes that: 'Privacy invasions are central to the business model of Internet platforms, devices and services: the more information they have about us, the more they have to sell to advertisers, data brokers, and governments, who can further exploit and control.'¹²⁷ The potential of what can be done with data and information advantage is expansive, including in relation to data's

¹²¹M Fineman 'Vulnerability and inevitable inequality' (2017) 4(3) *Oslo Law Review* 133 at 142.

¹²²*Ibid.*, at 142.

¹²³S Poppleton et al 'Who suffers fraud? Understanding the fraud victim landscape' (Victims Commissioner, 2021) p 4.

¹²⁴Sexual Offences Act 2003, ss 16–24.

¹²⁵See S Azmeh et al 'The rise of the data economy and policy strategies for digital development' (Digital Pathways at Oxford Paper Series No 10, 2021).

¹²⁶SM West 'Data capitalism: redefining the logics of surveillance and privacy' (2019) 58(1) *Business and Society* 20.

¹²⁷D Citron *The Fight for Privacy: Protecting Dignity, Identity and Love in Our Digital Age* (New York: WW Norton and Company, 2022).

predictive possibilities.¹²⁸ This marks a new era of fraud which is characterised by increasingly sophisticated attempts to entice people to share sensitive (often financial) information as the driving force for fraud.

(i) Fraud's lifecycles: outbound routes

This reappraisal of fraud's purposes can be further advanced through consideration of fraud's lifecycles, specifically fraud's outbound routes. While fraud may not lead to gain or loss in practice, focusing on fraud's outbound routes 'joins up' a conceptual account of fraud's meanings with fraud's operation in the real world. It is well known that the cashing out stage of fraud is significant in practice. Victims are concerned to recover losses they experience via fraud.¹²⁹ The Proceeds of Crime Act 2002 gives a framework for apportioning asset recovery in criminal law.¹³⁰ Civil law remedies, such as seizing and forfeiting money identified as proceeds, may operate concurrently to bring back funds to victims.¹³¹ Without this aspect in view, we do not have an explanation for pressures to disrupt fraud. Incorporating focus on fraud's outbound routes also joins up a conceptual account of fraud with the fact that victims of fraud are concerned with reimbursement. This is especially important where cryptocurrency is involved, given the fast and irreversible nature of these transactions.¹³² Considering outbound routes to fraud also gives a means of identifying fraud, especially as acquisition of information capital is difficult to identify.

What are the implications for conceptualising fraud's purposes? Even if data is brought within the scope of intangible property, there is now scope to make data acquisition and manipulation more central and explicit to fraud's purposes.¹³³ Information capital, information advantages and intangibles all need to be centralised within an account of fraud's purposes, alongside gain and loss in real property.

(c) Fraud's fault

Fault requirements, also known as *mens rea*, are a key element of criminal liability.¹³⁴ Fraud's core norms involving fault are acting deliberately and with dishonesty. Concepts of deliberateness and dishonesty are strongly linked to objective assessment of breach of trust. Of significance in reshaping these norms is the foothold for fraud provided by changes in accountability and governance structures. This includes changes in regulatory environments within the digitalised economy, which include voluntary and mandatory agreements in relation to fraud prevention and reimbursement.

We turn first to dishonesty. Dishonesty is a difficult term to define but is a key normative aspect of fraud. In criminal law, where a dishonesty direction is given, 'dishonesty' is to be assessed according to the standards of the ordinary and honest person, considering knowledge and belief of circumstances known to the accused.¹³⁵ We noted in unpacking industrialised fraud above that people are living increasingly virtual lives. This is accompanied by changes in the way we transact, with more transactions occurring online.

A digitalised society prompts fresh reflection on the contours of assessments about dishonesty. We can hypothesise that expectations of digitalised society exist, which means that it is to be expected that some content is not truthful. This arises because boundaries are increasingly blurred between what is real and what is not real. For example, it might now be seen as acceptable that social media companies allow exaggerated or untrue content on their platforms. Would the so-called 'Generation Z' assess as dishonest

¹²⁸D Citron and F Pasquale 'The scored society: due process for automated predictions' (2014) 89 Washington Law Review 1.

¹²⁹M Button et al 'Support for the victims of fraud: an assessment of the current infrastructure in England and Wales' (London: National Fraud Authority, 2009) pp 21–22.

¹³⁰See *R v Hunter; Smith* [2021] EWCA Crim 1785.

¹³¹G Virgo *The Principles of the Law of Restitution* (Oxford: Oxford University Press, 4th edn, 2024) ch 20.

¹³²For example, Coinbase.

¹³³H Karna 'Data is a "tangible" asset' (CFO, 2018) <https://www.cfo.com/news/data-is-a-tangible-asset/659035/>.

¹³⁴J Horder *Ashworth's Principles of Criminal Law* (Oxford: Oxford University Press, 10th edn, 2022) p 171.

¹³⁵*Ivey v Genting Casinos (UK) Ltd t/a Crockfords* [2017] UKSC 67; *R v Barton and Booth* [2020] EWCA Crim 575 at [109].

a misrepresentation that an influencer has 30,000 followers on Instagram, when the true number is much less? Expectations of total veracity in the online environment have changed, and there is a degree of acceptability around exaggerated social media content or reviews about products.¹³⁶

There is a convincing, albeit provocative, argument that there must be changes to an objective assessment of dishonesty within the framework of the digitalised economy. Normative standards of dishonesty are now mediated by expectations within the digitalised economy.¹³⁷ This will in turn influence the normative contours of fraud. The boundaries of dishonesty must be interrogated as part of principles of an equitable digital society.¹³⁸

A second point concerns deliberateness, which is linked to the accountability and governance foothold to fraud. This shapes an argument about what should be left *outside* of the normative core of fraud rather than what should be within it. Specifically, deliberateness is being reshaped by societal changes in tolerance and risk within the digitalised economy. The core of fraud will continue to place deliberateness centrally. However, it is also notable that individuals may be more willing to run the risk of being involved in fraud, as part of a network used to facilitate fraud. For example, there has been a recent surge in money mules amongst cash-strapped individuals, including university students and older adults who are feeling financially pressurised.¹³⁹ Mule accounts are used by fraudsters as an exit route to fraud. The most common form of money muling involves an individual (money mule) being offered cash to let a third party use their bank account to transfer money.¹⁴⁰ This allows fraudsters to channel proceeds of fraud through bank accounts which are not in their name. This blurs the boundaries between the fraudster and their target. This issue is intensified in situations involving crypto markets and click farms where large numbers of individuals and communities are drafted into fraudulent schemes.¹⁴¹

It is important to have sight of a network of enablers to fraud – potentially unknowing of their purposes within a fraudulent scheme – as part of the wider meanings of fraud. This may sit outside a core account of fraud, given the lack of knowledge in relation to the fraud itself. These networks nevertheless link strongly to organised economic crime groups reshaping fraud's meanings and can be contrasted with more opportunistic fraud.

Conclusion and implications for fraud criminalisation and regulation debates

There has been much written in fraud policy documents on the need to build a robust anti-fraud ecosystem and the need for agility in doing so.¹⁴² There have been numerous reports on fraud in the past five years since the start of the Covid-19 pandemic.¹⁴³ I have argued that the first step for those interested in the criminal law's principled development is to unpack just how dynamic fraud's meanings now are in

¹³⁶J Roozenbeek and S van der Linden 'Fake news game confers psychological resistance against online misinformation' (2019) 5 Palgrave Communications 65.

¹³⁷Acknowledging that this raises issues for people in the neurodiverse community, some of whom may interpret events and conversations literally.

¹³⁸See S Shapiro 'Collaring the crime, not the criminal: reconsidering the concept of white-collar crime' (1990) 55 American Sociological Review 346; B Bodo 'The commodification of trust' (Amsterdam Law School Research Paper No 2021-01, 2021); A Giddens *The Consequences of Modernity* (Stanford: Stanford University Press, 1990).

¹³⁹Barclays Bank 'Barclays warns of 23 percent surge in student money mules' (Barclays Press Office, 2023) <https://home.barclays/news/press-releases/2023/10/barclays-warns-of-23-per-cent-surge-in-student-money-mules/>; Cifas 'Latest fraud statistics reveal middle-aged mules targeted by online money laundering groups' (Cifas, 2021) <https://www.cifas.org.uk/newsroom/middle-aged-mules>.

¹⁴⁰National Crime Agency 'SARs in action: money mules' (UK Financial Intelligence Unit, 2023); Home Office *Money Mule and Financial Exploitation Action Plan* (HMSO, 2024).

¹⁴¹W Poster 'Introduction to special issue on scams, fakes, and frauds' (2022) 24(7) New Media and Society 1535 at 1538. National Crime Agency 'National Strategic Assessment (NSA) campaign – money laundering' <https://www.nationalcrimeagency.gov.uk/threats-2025/nsa-illicit-finance-2025>, estimates that over £10 billion is laundered annually via money mule activity in the UK.

¹⁴²For example, *Fraud and the Justice System*, above n 5, at [9].

¹⁴³Above n 5, reports cited.

the digital era. The industrialisation of fraud demands reframing of fraud's core norms within the digitalised economy through consideration of fraud's footholds and lifecycles.

Not everything that can be identified as 'fraud' should be considered criminal fraud. However, this work provides a firmer foundation for principled debate about fraud criminalisation and associated regulatory strategies, a matter of current importance. A new Fraud Strategy is expected from the Labour government.¹⁴⁴ Crucially, the conceptual work in this paper exposes the fundamental transnational nature of industrialised fraud. The industrialisation of fraud in practice, as seen in organised scam compounds in Southeast Asia and fraud centres in West Africa and India, reveals how fraud has become embedded in transnational economic structures.¹⁴⁵ Fundamentally international legal harmonisation is required, including shared definitions of fraud.¹⁴⁶

The first implication is that the industrialisation of fraud means that fraud cannot be designed out entirely within a digitalised economy using criminal and/or regulatory measures. When it comes to assessing justifications for criminal law and/or regulatory strategies, securing civil order (a key purpose of the criminal law) will demand calibration of risk and social tolerance in relation to fraud. There is a choice about how much fraud to 'allow' in certain spheres, with social practices likely to demand that this is set at a minimum level. Central cases of fraud as defined within criminal law proposals will be guided by an inward flow of ideas, based on an emerging consensus about the core of industrialised fraud. It must be determined what levels of fraud are tolerable in supporting civil order, as well as what responsibilities should remain with individuals. Analysis of the roles given to citizens, state and government in relation to fraud will cast light on the criminal law as an 'institutional normative order'.¹⁴⁷

Secondly, technological innovation is an inherent permanent feature of industrialised fraud such that the task of distinguishing cyber fraud, online fraud and other forms of fraud is largely redundant.¹⁴⁸ It is more productive for future fraud strategies to engage with understanding fraud's meanings within the digitalised economy. This involves identification and scrutiny of fraud's footholds and fraud's lifecycles as the digitalised economy expands and develops at pace. It also means that digital nomenclature needs to be embedded within fraud law scholarship, including AI-generated fraud; AI-enabled fraud; AI-dependent fraud; Big Tech; non-human technical systems (such as bots).¹⁴⁹

Given the well-known challenge of 'keeping up' with fraud in the real world, it is more intellectually honest to concede that fraud's meanings are less stationary and settled than previously assumed. Not only have there been changes to fraud's core *modus operandi* (for example, using generative artificial intelligence and deepfakes) but industrialised fraud is a concept built on, shaped by and embedded within the rapid changes and developments of the digitalised economy. This will be relevant in relation to upstream enablers to fraud, through use of Internet platforms, emerging technologies and in considering who is responsible for these technologies. This nomenclature is also relevant when considering the channelling away of the proceeds of fraud, facilitated by money mules and/or technologies which enable instant transfers.

Thirdly, a more dynamic understanding of fraud in a digital era casts fresh light on the limitations of criminalisation measures in preventing and addressing fraud. For example, once an in-principle case has been made for fraud criminalisation (based on serious wrongdoing and a harm threshold being passed),

¹⁴⁴The Rt Hon Lord Hanson of Flint 'Lord Hanson unveils ambitious new approach to tackling fraud' (27 March 2025) <https://www.gov.uk/government/news/lord-hanson-unveils-ambitious-new-approach-to-tackling-fraud>.

¹⁴⁵I Franceschini et al 'Compound capitalism: a political economy of Southeast Asia's online scam operations' (2023) 55(4) *Critical Asian Studies* 575; M Button et al *Scoping Study on Fraud Centres: Ghana, India and Nigeria* (Itad, 2024) <https://www.itad.com/wp-content/uploads/2024/11/Fraud-Scoping-Study-for-publication-2024.pdf>.

¹⁴⁶Cross, above n 105.

¹⁴⁷Farmer, above n 12, p 117.

¹⁴⁸S Dawda *Rethinking the UK Response to Cyber Fraud: Key Policy Challenges* (London: RUSI, 2020).

¹⁴⁹Europol, above n 6; B Martinez et al 'Mapping the state of the art: artificial intelligence for decision making in financial crime' in B Martinez et al (eds) *Cybersecurity for Decision Makers* (Boca Raton, FL: CRC Press, 2023).

further constraints or countervailing reasons not to criminalise need to be considered.¹⁵⁰ These include ensuring criminal law measures are appropriate and preferable to other state interventions. This paper has revealed the fundamental transnational aspect of industrialised fraud.¹⁵¹ Some central cases of industrialised fraud occur quickly, with proceeds channelled away quickly and irrevocably via cryptocurrency. Clearly, criminalisation is not well-suited to responding to transaction frauds undertaken at speed, assisted by Blockchain technologies. There are issues concerning varying definitions of fraud across jurisdictions, creating difficulties for enforcement which must be considered, alongside the use of extraterritorial jurisdiction against alleged fraudsters based in foreign countries.¹⁵²

Similarly, regulatory measures may create unfavourable incentive structures within the digitalised economy. As noted above, the banking industry is now responsible for reimbursing fraud victims through a Mandatory Reimbursement Model up to £85,000, currently overseen by the Payment Systems Regulator.¹⁵³ Empirical work is needed to establish whether individuals may be more tempted to take risks in relation to their money as a result. There are reduced downsides to responding to a favourable offer to double a pension fund, for example, if an individual knows that they will get any money fraudulently lost up to £85,000 back through mandatory reimbursement. This may affect risk appetite in the population towards fraud.¹⁵⁴ In practice, some regulatory schemes have the effect of blurring distinctions between intended victim/s of fraud and functional victim/s of fraud who become responsible for reimbursing the losses of fraud.

A more dynamic fraud criminalisation ecosystem, which takes into account the transnational nature of industrialised fraud, demands that arguments *against* criminalisation and/or regulation are robustly explored. Overall, this paper's suggested reframing of fraud's meanings highlights the need to stay abreast of developments in the digitalised economy as a key underpinning for robust legislative work on fraud. Digital futures are criminal law's futures, too.

¹⁵⁰RA Duff and S Green 'Introduction' in RA Duff and Stuart Green (eds) *Defining Crimes: Essays on the Special Part of the Criminal Law* (Oxford: Oxford University Press, 2005) p 9; JS Mill *On Liberty* (first published 1859, Harmondsworth, 1979). On the meaning of 'harm' see A von Hirsch and N Jareborg 'Gauging criminal harm: a living-standard analysis' (1991) 11 *Oxford Journal of Legal Studies* 1.

¹⁵¹Cryptocurrency is inherently transnational, lacking central jurisdiction.

¹⁵²C Ryngaert *Jurisdiction in International Law* (Oxford: Oxford University Press, 2nd edn, 2015) pp 110–113.

¹⁵³PSR 'Consolidated policy statement: APP scams reimbursement requirement' (May 2025) <https://www.psr.org.uk/media/rhylv4op/ps25-5-app-scams-reimbursement-consolidated-policy-statement-may-2025.pdf>.

¹⁵⁴Including psychological distress caused by fraud or repairing credit rating, involving time and money.