STUART BIGGS

OTHER PEOPLE'S CRIMES

Thoughts on approaches to financial crime prevention and the internet

MARCH 2023

PUBLISHED BY

cloth fair

CHAMBERS

Introduction

Our traditional concepts of culpability and criminality are being challenged in today's digital world, and the Online Safety Bill that is working its way through parliament has the potential to effect significant changes for regulators, individuals and corporates alike. We are therefore pleased to recommend this paper by Cloth Fair's most recent member, Stuart Biggs, which highlights some of the key issues and offers a thought-provoking analysis of the Bill from a financial crime perspective.

The author

Stuart Biggs joined Cloth Fair Chambers in November 2022 and is a highly ranked junior in financial crime. He advises on a range of matters affecting companies including bribery, fraud, anti-money laundering, sanctions, data protection, brand and content protection, advertising regulation and consumer protection. He is recognised in particular for his expertise in cases involving allegations of investment fraud and in regulatory and criminal proceedings involving the FCA. Over many years he has advised rightsholders in respect of online Intellectual Property Crime. He assists corporates with internal investigations relating to regulatory and/or criminal matters and in their interactions with the criminal justice system.

LINKS

> **Stuart's CV**

STUART BIGGS

OTHER PEOPLE'S CRIMES

Thoughts on approaches to financial crime prevention and the internet

ABSTRACT

This article considers the duties of care imposed by the Online Safety Bill in the context of other laws that have imposed criminal and/or civil liability on businesses whose services are misused by their customers to commit crimes. It considers the basis for imposing obligations and the difficulties in balancing competing rights to conduct business as well as rights of expression. Acknowledging there are no perfect answers here, the article considers the problems presented by both criminal law and regulatory systems. The Bill should be seen in the wider context of the failure to prevent approach with the concomitant questions as to how it meets our traditional concepts of culpability and criminality and older distinctions between acts and omissions. The article concludes with a look to the task of the regulator in finding the balance over the coming months and, in particular, to the role for the industry in that process.

A short walk from what is now the construction site of London's forthcoming Fraud and Cybercrime Court, the Aldwych farce *It Pays to Advertise* opened in 1924 and made comedy of the idea that people would rush to buy *"The most expensive soap in the world!",* readily assuming those placing the advertisement had in fact any soap.

Fraudulent advertisements, both paid-for content and user-generated promotions, are among the targets of the Online Safety Bill; an example of the ways in which the services provided by online companies in the course of their ordinary businesses, facilitate the commission of crime. The internet provides the infrastructure for modern life but the spaces within it are privately owned and difficult to patrol.

In their Fraud Update for the first half of 2022, UK Finance wrote:

> *"Scammers are also increasingly using social media sites to entice victims by advertising fake investments, such as crypto currency schemes or gold or property. In some cases, social media 'influencers' may be used to promote such schemes and create an air of legitimacy."*

Although the total number of frauds recorded has reduced as against the Pandemic period, which saw a huge increase in online fraud, there is a clear trend that fraud by authorised payments is going up; more people are being scammed[1].

Staring Cnut-like at a tidal wave of digital fraud and other online harms, one can understand governmental and parliamentary motivation to pass responsibility to tech companies. As has long been observed, policy makers seek out *"pinch points"* where law and regulation are most likely to achieve their objectives; identifying situations in which the application of regulatory action to an identified few can have a controlling effect on the activities of many others[2].That utilitarian argument is supplemented by a populist one: the internet companies make a lot of money, they *ought* to bear the cost of preventing others from misusing their services. How though should the law address the question of the *culpability* of companies which do not endorse criminal activity and indeed would rather their criminal customers stay away?

In its report, *Fraud and the Justice System*, published on 18 October 2022, the House of Commons Justice Committee stated:

1 Half year fraud update 2022.pdf (ukfinance.org.uk)

2 C Reed 'Policies for Internet Immunity' (2009) 19(6), Computers and Law, 20

We acknowledge that telecommunications and tech companies are taking steps to improve their response to fraud, however they remain platforms through which the majority of frauds impacting the general public are conducted. There still appears to be a lack of engagement on this subject from those sectors, not least amongst the telecommunications companies. Fraudsters may be using increasingly sophisticated technologies and methodologies to conduct their crimes but we are not convinced that the largest companies in those sectors do not have the capabilities to increase their efforts to tackle these changes and prevent frauds, particularly in paid-for-advertising, from appearing on their systems. Fraud may not have a significant impact on the bottom-line of those companies, however they have a duty of care to their users to ensure everything possible is being done to design frauds out of their systems in order to protect the public.

…

The 'failure to prevent' offence for bribery has had success in driving better corporate behaviours. A similar offence for failure to prevent fraud being perpetrated using a company's platforms would not only aid prosecution for these failures but focus private sector effort on designing fraud out of companies' systems. A failure to prevent fraud offence should be introduced to hold companies to account for fraud occurring on their systems and encourage better corporate behaviours."[3] [emphasis added]

The language of the Committee is confrontational and those who operate tech and telecoms companies will be on guard. In January 2023 the Government faced what was described as a backbench rebellion over the lack of criminal liability for tech executives in the Bill. Whilst that was quelled in a way that resulted in what is a rather limited amendment to the Bill,[4] the wider question as to what extent companies and executives should face criminal conviction for failing to prevent the crimes of others will not disappear.

In the above paragraphs of their report, the House of Commons Committee asserts: that companies have duties to prevent the crimes of third parties; that those are duties to do *everything possible* as opposed to that which is reasonable and proportionate (perhaps that can be passed over as hyperbole); and that the failure to prevent model might be expanded beyond liability for the acts of associated persons, the limitation in the Bribery Act 2010, the Criminal Finances Act 2017 (in respect of tax evasion) and in the proposed amendments to introduce offences of failing to prevent fraud, fraudulent accounting and money laundering into the Economic Crime and Corporate Transparency Bill, to encompass the acts of people who use the corporate's *systems*.[5]

We can consider the Online Safety Bill alongside the wider development of the failure to prevent model because they both concern the question of the extent to which companies, and ultimately executives, are to be made responsible for failure to put sufficient measures in place. Indeed, the former Minister for Technology and the Digital Economy, Damian Collins MP told the House of Lords' Fraud Act 2006 and Digital Fraud Committee that the

3 Paras 136 and 145

4 An offence of failing to prevent non-compliance by the company with an information request.

5 On that third point, in producing its own report the following month, the House of Lords Committee on the Fraud Act and Digital Fraud, noted, the Commons Committee "appeared to suggest" the concept of failure to prevent should be expanded in that way: HoL FA 2006 and Digital Fraud Committee report, para. 513.

"You know, you can do this just as easily online."

provisions in the Online Safety Bill translate to *"a failure to prevent the facilitation of fraud offence by proxy"*.[6]

It might be better to recognise this as being goal driven utilitarian law-making rather than to suggest, as the Justice Committee have done, that it is grounded in a pre-existing duty to prevent others misusing or taking advantage of one's service for a criminal end. The Online Safety Bill imposes duties rather than divining them.

As discussed below, an alternative analysis, that internet service providers necessarily have some form of ownership of or strict liability in respect of everything that is delivered to their users, is counter to the established approach to the operation and development of the internet.

There is a different attitude to fraudulent advertisements in the hardcopy media. There are of course advertising codes, but the hard copy newspaper which prints a fraudulent advert will not be liable. The focus of ASA is instead the marketer, as is the focus of the FCA for financial promotions in print. In the US, the Federal Trade Commission provides guidance to help media outlets assess the advertisements they run[7] but the view reflected in law, is that newspapers publishing online are not well placed to assess claims made in advertisements

6 Ibid. para 515

7 Screening Advertisements: A Guide for The Media | Federal Trade Commission (ftc.gov)

and they are not liable unless they provide an endorsement, notwithstanding that a consumer may get some level of subconscious reassurance from the fact that something is advertised in a major newspaper.

Newspaper advertising has always been given a degree of latitude; concern with consumer protection being entangled with concerns for the protection of the free press and free speech. As Price and Verhulst observe in Self Regulation and the Internet[8], it was because television was considered more *pervasive, invasive and influential* within society than any other medium that regulation of broadcasting was called for and justified.

The internet, and in particular social media, are certainly pervasive and there is undoubtedly public support for legislative reform and control because there is such scope for harm. Of course, the flipside, is that the quantity of material carried on sites is so many times greater that its content could never be manually checked[9].

CIVIL LAW AND DUTIES

There is a divergence between the public and private law positions which suggests there is not a clear inherent basis for the imposition of responsibility. Mere facilitation and even knowing assistance are not sufficient to establish joint tortfeasorship[10], which is a narrower concept than that of criminal secondary liability. The position in defamation is that an internet service provider that performs no more than a passive role in facilitating postings on the internet cannot be deemed to be a publisher at common law and will be protected under the Defamation Act 1996 until on notice[11].

In tort the distinction is made between the concept of complicity and the idea of a duty to take care to prevent harm. In *Robinson v Chief Constable of West Yorkshire Police* [2018] AC 736 the Supreme Court reiterated that individuals and bodies are generally under no duty to prevent harm and cited with approval the following passage from Tofaris and Steel, "Negligence Liability for Omissions and the Police" [2016] CLJ 128:

> *"In the tort of negligence, a person A is not under a duty to take care to prevent harm occurring to person B through a source of danger not created by A unless (i) A has assumed a responsibility to protect B from that danger, (ii) A has done something which prevents another from protecting B from that danger, (iii) A has a special level of control over that source of danger, or (iv) A's status creates an obligation to protect B from that danger."*

Robinson was followed in the case of *Al-Najar v. Cumberland Hotel (London) Ltd* [2019] EWHC 1593 (QB) which directly addressed the question as to what extent a company is liable for the criminal act of a third party. Hotel guests were subjected to a violent attack by an intruder who gained access after the guests left their door on the latch. Dingemans J held that the hotel had assumed a responsibility to protect its guests. It was a duty to take reasonable care to protect against the risk of attacks which

8 Kluwer Law International

9 See the arguments currently advanced by Google to the Supreme Court in the US: 20230112144706745_Gonzalez v. Google Brief for Respondent - FINAL.pdf (supremecourt.gov)

10 Sea Shepherd UK v Fish & Fish Ltd [2015] UKSC 10

11 Bunt v. Tilley [2006] EWHC 407 (QB); Tamiz v. Google Inc [2013] EWCA Civ 68

meant the particular attack was not a break in the chain of causation. On an assessment of the hotel's security measures, the Court held there was no breach of that duty. The same outcome had been reached, by a different route, by the Court of Appeal in Everett v Comojo [2011] EWCA Civ 13; [2012] 1 WLR 150, in respect of a stabbing in a nightclub.

Attempts to draw analogies between tech companies and businesses in the physical world like hotels or, as the Justice Committee did with banks, risk oversimplification, both in terms of the assessment of proportionate measures and moreover, in terms of the foundations for the assertion of a duty of care. That said, the assumption of responsibility by a hotel for the safety of its guests or a bank for the protection of customers' money, is quite different from the acceptance of responsibility of most sites to their users[12].

SAFE HARBOUR

The concept of making tech companies responsible for preventing crime needs to be seen against the background of an existing regime designed to encourage the commercial development of the internet and to protect internet companies.

Internet service providers (a broadly defined term) have the benefit of a bespoke level of protection, albeit one with limitations. The E-Commerce Directive provided *safe harbour* defences for internet service providers, including companies such as YouTube, Google and Facebook, concerned in the caching or hosting of illegal content, or which provide a mere conduit for digital material.

Those defences recognise a positive public and economic interest in the development of the internet. They were incorporated into UK law by Regulations 17 to 19 of the Electronic Commerce (EC Directive) Regulations 2002, so that, for example, Regulation 19 states:

> *19. Where an information society service is provided which consists of the storage of information provided by a recipient of the service, the service provider (if he otherwise would) shall not be liable for damages or for any other pecuniary remedy or for any criminal sanction as a result of that storage where—*
> *(a) the service provider—*
> *(i) does not have actual knowledge of unlawful activity or information and, where a claim for damages is made, is not aware of facts or circumstances from which it would have been apparent to the service provider that the activity or information was unlawful; or*
> *(ii) upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information, and*
> *(b) the recipient of the service was not acting under the authority or the control of the service provider.*

The Directive contains, at Article 15, a prohibition on general obligations to monitor. This was never a prohibition on requirements for a site to monitor for content that was specifically identified[13] and the recitals to the Directive spoke of limitations to the prohibition including the possibility of

12 The unique position of banks is reflected in the recent decision of Philipp v Barclays Bank UK Plc [2022] EWCA Civ 318 in which the Court recognised a bank has a duty of inquiry where it has relevant reasonable grounds for belief that a customer's request to make an electronic payment from their account may result from a fraud being committed against that customer.

13 See Peterson v Google LLC (C-682/18)Elsevier Inc v Cyando AG (C683/18) and the opinion of the Advocate General in Glawischnig-Piesczek v Facebook Ireland Ltd (C-18/18)

member states imposing *duties of care to detect and prevent certain illegal activity*[14], but the general principle was that sites should not be required to monitor everything that was visible to their users. Post Brexit, Article 15 of the directive, which was not included in the domestic regulations, falls away.

Meanwhile the EU's Digital Services Act, published on 19 October 2022, states at recital 30,

> *"Providers of intermediary services should not be, neither de jure, nor de facto, subject to a monitoring obligation with respect to obligations of a general nature. This does not concern monitoring obligations in a specific case and, in particular, does not affect orders by national authorities in accordance with national legislation, in compliance with Union law, as interpreted by the Court of Justice of the European Union, and in accordance with the conditions established in this Regulation. Nothing in this Regulation should be construed as an imposition of a general monitoring obligation or a general active fact-finding obligation, or as a general obligation for providers to take proactive measures in relation to illegal content."*

The distinction between specific and general monitoring is not clearly drawn and seems to be left as a matter for the CJEU,[15] a further example of putting off the battle between different rights under the EU Charter which include the rights to conduct a business as well as rights of free expression[16].

14 See Recitals 47 to 49

15 See Alexander Peukert and others, 'European Copyright Society: Comment on Copyright and the Digital Services Act Proposal' 367; and see discussion in TAKING FUNDAMENTAL RIGHTS SERIOUSLY IN THE DIGITAL SERVICES ACT'S PLATFORM LIABILITY REGIME, Giancarlo Frosio and Christophe Geiger, European Law Journal 2022

16 Articles 16 and 11 of the EU Charter of Fundamental Rights

The caselaw in respect of safe harbour, in the field of intellectual property, has largely turned on the nature of the site and the extent to which it is involved in courting a particular type of content[17]. There is perhaps an increasingly important distinction to be drawn as to whether sites thrive because of the access they provide to illegal content, because certain types of illegal content - copyright breaches and types of hate speech as examples - increase traffic. For some sites it is a point of concern, for others it is to one extent or another, part of their business model, so that there is a sense of what may be said to be 'common enterprise'[18].

THE OVERLAP WITH CRIMINAL SECONDARY LIABILITY

The criminal law of secondary liability has developed so as to exclude any requirement of motive or common enterprise. In the commercial context, it is a close cousin of the failure to prevent model, sharing in its most recent statutory form a defence of reasonableness which amounts here to an assessment of reasonable measures.

National Coal Board v. Gamble [1959] 1 QB 11 (1958) established the law in respect of aiding and abetting in a commercial context. A commercial entity may be guilty of aiding and abetting an offence where there is a positive act of assistance voluntarily done, and a knowledge of the circumstances constituting the offence. That decision was not without controversy, as evidenced by the dissenting judgment of Slade J in which he argued that the question of motive on the part of the aider and abettor was relevant. Slade J considered there had to be some sort of

17 See, for example, the Pirate Bay and the cyberlocker litigation

18 A phrase used by C Reed, 'Policies for Internet Immunity' (2009) 19(6), Computers and Law, 20

commonality of enterprise to separate the provision of assistance coincidentally in the course of one's ordinary business from what he saw as the truly criminal act.

After *NCB v Gamble*, there remained the view that there should be some limitation on criminal accessory liability based upon culpability. In 1972 a very distinguished Law Commission working party[19] set out General Principles on *"parties, complicity, and liability for the acts of another"* and their proposition 6(4) was: *"A person who is in a position to prevent an offence, because he is in control of property or for some other reason, is not to be taken to be an accessory merely because he fails to prevent an offence."* They concluded that there, *"may be a case for special provisions in certain contexts to penalise a person in a position of responsibility who permits another to commit an offence, but this ought not to affect the general principle in the present sub-paragraph."* The possible exception of the person who gives some sort of implied permission from a superior position was tightly constrained.

Subsequent developments eroded the distinction between acts and omissions. Indeed, in the present context, the distinction lacks substance where the positive act is not particular to the commission of the offence but simply the continuation of a service provided universally to all customers.

In 1993 the Law Commission proposed a revised codification of the law of assisting and encouraging crime. The Commission was of the view that positive action should be an element of the offence *"rather than a mere failure to discharge a legal or moral duty to control another, or a failure to exercise authority to prevent criminal conduct"* because it would be *"too burdensome"* to impose *"what would in effect be obligations of law enforcement"*.

The example was given of the landowner who has legal authority to order off his land trespassers who are using it to engage in illegal trading.[20] However, the Commission concluded that where there was a positive act, there would be no exception for the defendant who provided assistance in the ordinary course of trade. The authors of the Consultation Paper noted:

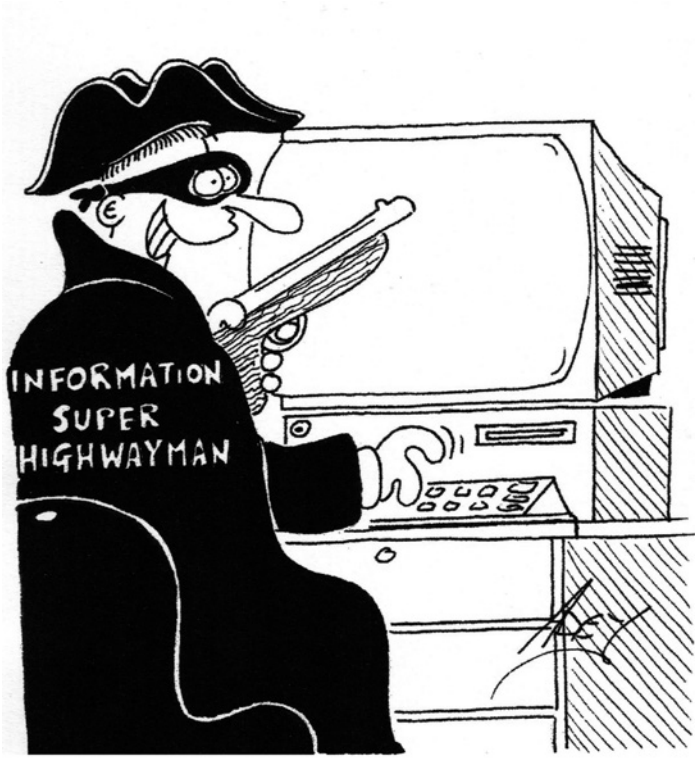
> *"A type of case that is frequently cited as needing to be excluded from complicity liability is that of "ordinary business supply. Thus, the taxi-driver who takes a fare to the scene of the crime; the Coal Board that in NCB v Gamble supplied the coal that constituted the illegal load; and the wholesalers who sell goods to DIY companies who are going to retail them on Sunday; all are actually or very arguably guilty of complicity under the present law"*

The Commission was of the view that setting the mental element of the new offences at belief rather than suspicion would draw the line in the appropriate place:

> *" … A balance has to be struck between the social interest in inhibiting crime by cutting off its materials and the social and personal interest in not unduly inhibiting the conduct of business by the imposition of criminal sanctions. Once belief as to the principal's criminality is required on the part of the supplier, he would seem to place himself in a position where the public interest in crime*

19 Scarman J, Derek Hodgson QC (later Hodgson J), Norman Marsh QC, Davies LJ, the Common Sergeant, Professor Glanville Williams were some of the members.

20 Assisting and Encouraging Crime An Overview, Law Commission, Law Commission Consultation Paper No. 131, 1993



prevention should prevail, if he continues to supply in those circumstances … For our part, though we invite comment, we see great difficulty in any suggestion that, within the context of a properly limited law of complicity, those who otherwise fulfil the requirements of that law should be excused because they act for mercantile or financial motives. Indeed, from the point of view of discouraging or inhibiting the commission of the principal crime, it might be thought desirable that "business" suppliers, above all others, should be deterred from providing the means of crime."[21]

This, understandably perhaps given the historical perspective, seems to look at supply as a one-off act with peculiar circumstances and pause for reflection.

The Law Commission returned to the 1993 consultation in its report in 2006 and concluded that there should be a general reasonableness defence but no special defence for the *"indifferent assister whose facilitative act was done in the ordinary course of a business"*[22].

This was followed by the creation of Part 2 of the Serious Crime Act 2007 in which, consistent with the Law Commission's recommendation, there were created new substantive offences of assisting and encouraging crime amongst which the minimum mental element is belief.

21 4.113-4.116, Law Commission Consultation Paper No. 131

22 6.50, Inchoate Liability for Assisting and Encouraging Crime, Law Com No 300

The Act provides a defence of acting *reasonably* in section 50 and section 47(8) defines the doing of an act to encompass failing to act and the continuation of an act already begun, killing off the distinction between acts and omissions and any debate as to what might constitute a *pure* omission.

There is also an absence of any de minimis principle, as noted by K.J.M. Smith with the lovely example of the shopkeeper who puts himself in jeopardy under the Act by selling P a pair of gloves after P has confided that they would make his forthcoming winter season of bicycle stealing *"much more comfortable"*.[23] Note that the majority of the Supreme Court in the Sea Sheppard case applied a de minimis principle in formulating joint tortfeasorship.

The Part 2 offences have been the subject of academic and judicial criticism and have also been largely avoided by prosecutors. We have not then had many opportunities to see how juries view the defences of the Law Commission's *trader who can prove that he or she acted reasonably in the circumstances*.

There are similarities here with the offences of failing to prevent bribery and tax evasion and the further examples being proposed as amendments to the Economic Crime and Corporate Transparency Bill where there are variously defences of having had in place adequate procedures or such procedures as it was reasonable to have (if any).

Those offences all relate to the acts of associated persons rather than third party customers/service users, which is why the Justice Committee's suggestion that a failure to prevent offence be extended to encompass any fraud using a company's systems is particularly remarkable. What is reasonable to expect in relation to employees and agents may be very different from what is reasonable as protection from strangers.

The Bribery Act has been for force for some time now but there may only have been one trial in which a jury has been asked to assess the adequacy of steps taken to prevent bribery.[24] One cannot blame prosecutors for not wanting to litigate reasonableness but the position for defendants is no more reassuring.

This is the cul-de-sac the draftsperson arrives in when trying to codify the balance between commercial freedom and obligations to prevent crime. A law which says that conduct is criminalised save where it is reasonable such that it does not justify criminalisation, can be frustratingly circular.

The task of assessing reasonableness involves the assigning of weight to competing interests and compromise. Some instances of criminality will be self-evident and/or so serious that the proportionate response will be clear. In many other cases, particularly in respect of fraud and the advertisement of financial products, it will be a much more nuanced question. This is fuzzy law that risks acting retrospectively in instances where there is genuine uncertainty as to whether a particular measure is reasonable.

That must surely be even more the case where there is scope for disagreement as to whether technological measures, such as filters and algorithms for use by websites, are efficacious or whether their cost is proportionate to their degree of efficacy or to the size of the business concerned.

23 The Law Commission Consultation Paper on complicity: Part 1: A blueprint for rationalism, Crim. L.R. 1994, Apr, 239-251

24 R v Skansen Interiors Ltd (Southwark Crown Court, March 2018)

Moreover, a test of reasonableness merges the distinction between the criminal law and the role of the regulator as courts are asked to look to guidance and codes of practice prepared outside Parliament to establish the *accepted* requisite standard.

THE MONEY LAUNDERING EXPERIENCE

Money Laundering is surely the field in which the obligation on people in business to take steps to detect and prevent the crimes of others is most well established and accepted. Anti-money laundering compliance is governed by offences of failing to report suspicions of crime as well as offences of failing to comply with due diligence requirements. This has revolutionised the financial services industry and the professions, and the enormity of that change and the specific justifications for it should be considered before it is transposed into a different context.

There is of course no general obligation to report crime. Prior to the Criminal Law Act 1967 a person committed the indictable misdemeanour of misprision of felony when, knowing that a felony has been committed and having a reasonable opportunity to disclose his knowledge, they did not inform the authorities of all material facts known to them. At that time there was no requirement that the concealment should be for the material benefit of the accused nor that it should consist in a positive act; it was a universal obligation[25]. After the passing of the Act, there was no offence unless information was withheld in return for payment.[26] In modern times the introduction of obligations to report require justification.

25 Sykes v. DPP [1962] AC 528
26 S.5 Criminal Law Act 1967

There came a point in time when it began to be accepted that the banking industry merited special treatment. In June 1980, the Committee of Ministers for the Council of Europe recommended that *"... the banking system can play a highly effective preventive role while the cooperation of the banks also assists in the repression of such criminal acts by the judicial authorities and the police"*.

In December 1988 the Basel Committee on Banking Regulations and Supervisory Practices, made up of representatives of central banks and supervisory authorities of member countries of the Group of Ten recognised, *"Public confidence in banks, and hence their stability, can be undermined by adverse publicity as a result of inadvertent association by banks with criminals. In addition, banks may lay themselves open to direct losses from fraud, either through negligence in screening undesirable customers or where the integrity of their own officers has been undermined through association with criminals. For these reasons the members of the Basle Committee consider that banking supervisors have a general role to encourage ethical standards of professional conduct among banks and other financial institutions."*

To that end the Basel Committee set out a statement of five principles accepting a degree of responsibility. Previously, the approach had been that banks had responsibility for their financial stability but not responsibility for oversight of the legitimacy of individual transactions.

Citing the Committee of Ministers and the Basel Committee in the recitals, the European Union adopted the first anti-money laundering Directive in 1990 which

imposed the requirement that credit and financial institutions and certain other professionals examine transactions, keep records and cooperate with law enforcement recognising that *"… preventing the financial system from being used for money laundering is a task which cannot be carried out by the authorities responsible for combating this phenomenon without the cooperation of credit and financial institutions and their supervisory authorities…"*

The Money Laundering Regulations 1993 implemented the Directive, Regulation 5 creating an offence of failing to maintain anti-money laundering procedures. At the same time the Criminal Justice Act 1993 introduced the offence of failing to report, the precursor to the s.340 offence in the Proceeds of Crime Act 2002. The broader but distinct concept of defensive disclosures had been introduced by the Drug Trafficking Act 1986 and the Criminal Justice Act 1988.

The anti-money laundering provisions developed to criminalise breaches of the specific requirements of the regulations. Further, the courts were directed to have regard to the guidance produced by the regulator in the interpretation of the regulations.[27]

The end position is a two-track system in which financial institutions may be convicted and fined - as NatWest was in 2021 for £264m - or given a civil penalty – as Santander was in December 2022 for £107m.

HEALTH AND SAFETY

Analogy has been drawn between the Online Safety Bill and Health and Safety legislation in support of transposition of commercial obligations into this new context.

Section 3 of the Health and Safety at Work etc Act 1974 provides *"It shall be the duty of every employer to conduct his undertaking in such a way as to ensure, so far as is reasonably practicable, that persons not in his employment who may be affected thereby are not thereby exposed to risks to their health or safety."* The defendant bears a legal burden of proof in respect of the best practical means to satisfy the duty[28]. Specific regulations such as the Regulatory Reform (Fire Safety) Order 2005, impose overlapping obligations.

The rationale for the creation of health and safety offences is in truth rather different to the matter in issue. For the most part, the provisions are focused on (physical) harm

and not primarily on crime. They are intended to address negligence, accident and the inherent danger in certain activities. Precautions to be taken in respect of the risk of accidental fire will to a large extent overlap with the reasonable response to the risk of criminal acts by third parties, such as arson or vandalism. This makes the analogy with the Online Harms Bill unconvincing.

ILLEGAL IMMIGRATION

A variation of the failure to prevent model appears in the Immigration and Asylum Act 1999 which provides a civil

27 See for example Reg 86(2) of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017.

28 S.40 Health and Safety at Work etc Act 1974; and see R v. AH Ltd [2021] EWCA Crim 359

penalty regime for transport companies who carry illegal immigrants into the UK. The failure to prevent type defence provides that the transport company must show that:

(a) he did not know, and had no reasonable grounds for suspecting, that a clandestine entrant was, or might be, concealed in the transporter,

(b) an effective system for preventing the carriage of clandestine entrants was in operation in relation to the transporter; and

(c) that on the occasion in question the person or persons responsible for operating that system did so properly.[29]

There is an applicable Code of Practice providing guidance. The application of that provision was considered by the Court of Appeal (Civil Division) in Bolle Transport BV v. Secretary of State for the Home Department [2016] EWCA Civ 783. The Court found that the system might involve the conduct of checks by a third party and that there could be a contractual indemnity for the penalty[30] if on the occasion in question the third party was at fault. Were the same approach to be applied to a criminal provision that would of course mean potentially a criminal conviction for strict or vicarious liability for the combination of the contracting party's failure and the unlawful behaviour of the stowaways.

In *International Transport Roth GmbH and another v Secretary of State for the Home Department* [2003] QB 728 the Court of Appeal considered the same statutory scheme.

Two aspects from the judgments are of interest to the question in hand. Simon Brown LJ found that the question for the Court was whether the scheme was *"not merely harsh but plainly unfair so that, however effectively that unfairness may assist in achieving the social goal, it simply cannot be permitted?"*

As the case turned on the application of Article 6, the Court considered whether the proceedings and penalty were properly classified as civil rather than criminal (for the purposes of the application of Article 6) and the fairness of a reverse burden to prove the deployment of reasonable measures to prevent the crime. Simon Brown LJ noted *"… surely a state can no more escape criminal classification and thereby the protections of Article 6 by artificially separating out a defence from the substance of the allegation, than by classifying offences as "regulatory" instead of criminal — held ineffective by the ECtHR in Ozturk -v- Turkey (1984) EHRR 409".*

Perhaps the most interesting aspect for present purposes was the partially dissenting judgment of Lord Justice Laws who devoted some of his reasoning to the identification of the essence of criminal law. He found that *the paradigm of a criminal law is one whose purpose is to condemn conduct perceived by the community at large as inherently wrongful.*[31]

He went on to identify the object of the legislation which was to engineer a reduction in offending, regardless of the culpability of any particular transport company and notwithstanding the language used in Parliament to condemn companies that failed to prevent the crime: [para 95]

29 S.34(3) IAA 1999

30 See paras 39 and 46

31 Para 92

… I think it is entirely obvious that the Crown's concern in seeking this legislation from Parliament, and Parliament's concern in passing it, was to prevent clandestine illegal migrants from entering this country, pure and simple. The purpose of the legislation is to achieve this end so far as possible. Whether such a migrant is let in by the negligence or connivance of a lorry-driver or owner is neither here nor there in terms of the vice the scheme is aimed at. The problems his entry creates are not bigger or smaller according to who let him in, or how, or whether he could have been stopped. The fact that honesty and due care on the part of those who own or drive the transporters will not stop the most determined entrants is neither here nor there to the purpose of the scheme. The deterrence of dishonesty and carelessness is not at the heart of it at all. Statements in Parliament about such matters, inevitably possessing the rancour and asperity of political utterance in a vigorous democracy, do not shift the reality of the Act's purpose.

96.. The nature of the scheme as I have described it stands, in my judgment, in stark contrast to the archetypal criminal case, where what is sought to be prohibited is the doing of

an act which is made inherently wrongful by its being done with a guilty mind. Take the crimes of theft and robbery. Society has no general interest in prohibiting the taking of one man's property into the hands of another, for that may be done by a gift, by a contract, by a will. But when it is done dishonestly — theft, or by violence — robbery, society intervenes with all the force of the criminal law. The vice is the dishonesty, the violence. Take next the calendar of sexual crimes. Leaving aside the rights and interests of children it is not society's business to interfere by the bludgeon of the criminal law with consensual sexual relations. But when one person's sexual attentions are forced on another, who is to the perpetrator's knowledge unwilling to receive them, the criminal law is at once and rightly engaged, from the case of a minor indecent assault to the offence of rape. Even the taking of life is not condemned simpliciter by the criminal law. Murder requires an intention to kill or do grievous bodily harm. Manslaughter requires proof of fault, of which various different kinds
may qualify.

97.. All these offences are archetypes of crime — the very idea of crime — in our law. They attract the condemnation of society because they are inherently wrongful. They are therefore rightly dealt with by the imposition of retributive punishment. But ideas of that kind simply have nothing to do with the reasons for putting in place the scheme of the 1999 Act. The statute is not interested in obloquy, shame or guilt. It is not interested in retributive justice. The scheme is put in place, and put in place only, as a means towards the fulfilment of the executive's particular responsibility to secure the State's borders by effective immigration control…"

Laws LJ concluded that the scheme under the 1999 Act was civil in nature for the purposes of Article 6. He was in the minority of the Court in that regard, but his analysis of the utilitarian objective of the legislation, the distraction of attempts to find moral turpitude on the part of the corporate entity that fails to prevent, and the consequent appropriateness of a civil response is thought-provoking and brings to mind by contrast the language used currently about tech companies.

In giving the third judgment, Lord Justice Jonathan Parker noted with approval the *entirely legitimate* aim of Parliament in minimising the role of the Courts in the enforcement of the Act. A similar regulatory approach is now pursued in the Online Safety Bill.

REGULATORY APPROACHES AND THE OSB

The common purpose of most regulatory regimes is to ensure that the commercial entity carries out its activity in question in a manner that is safe. Items for sale, from food and drink to financial products, must be safe for consumers, sold sometimes only to appropriate sections of the population, with appropriate warnings and fair descriptions.

Distinguishable from that concept is the more controversial idea of a regulation that requires a corporation to take actions to prevent, or at least obstruct or deter, the criminal act of a third party.

I have discussed above the unique position in respect of money laundering; the extent to which that approach applies in respect of health and safety and the way in which it is approached, as a civil rather than criminal law matter,

in respect of the carriage of illegal immigrants. The newest category is to be the operation of online user-to-user and search platforms under the provisions of the Online Safety Bill which will undoubtedly soon become law.

The Bill applies to all such services which are targeted at UK customers, those used by a substantial number of UK customers and those which might be used by UK customers where there is a risk of significant harm to individuals. It creates duties of care for operators of user-to-user and search services in respect of illegal content, which is defined to include content amounting to fraud, financial services offences or money laundering. It also contains obligations for certain tech services in respect of the proliferation of fraudulent advertisements.

For example, Part 3 of Chapter 5 of the Bill would impose duties on providers of certain user-to-user services and search services relating to fraudulent advertising. Providers must operate their services using proportionate systems and processes designed to:

(a) prevent individuals from encountering content consisting of fraudulent advertisements in or via search results of the service;
(b) if any such content may be encountered in or via search results of the service, minimise the length of time that that is the case;
(c) where the provider is alerted by a person to the fact that such content may be so encountered, or becomes aware of that fact in any other way, swiftly ensure that individuals are no longer able to encounter such content in or via search results of the service.

Fraudulent advertising is defined by reference to various Fraud Act, FSMA and Financial Services Act offences, although for reasons I have not been able to divine, not s.3 Fraud by failing to disclose information. Requirement (C) is similar to the safe harbour requirements, discussed above, and may be uncontroversial. The other requirements are more obviously challenging and involve monitoring.

The safe harbour defences remain[32] but the Online Safety Bill sidesteps them by creating liability not for the underlying unlawful material but on the basis of a freestanding obligation to put measures in place which might have prevented the occurrence of the content. This is the same distinction discussed above in respect of the law of tort.

The scheme is regulated by OFCOM. In summary, OFCOM will produce Codes of Practice and will review action taken by sites. OFCOM is to issue notices to require sites to implement particular measures, to issue fines for noncompliance and, ultimately, to apply for court orders to restrict the provision of services.

Yet the involvement of the criminal law is limited to backing up OFCOM's powers to require information and to conduct compulsory interviews and searches. There will likely be very little criminal litigation and most of that which there is will likely be relatively minor.

That avoids the creation of serious 'white elephant' offences[33] and it avoids juries grappling with questions of reasonableness. However, it also places a lot of power in

32 Confirmed in the Government response to the Online Harms White Paper

33 A term used by Mark Steward of the FCA with reference to some of the failure to prevent offences in providing oral evidence to the Fraud Act 2006 and Digital Fraud Committee on 26 May 2022 (pg 14 transcript)

the hands of the regulator. There will be fines based upon an assessment by the regulator of compliance and seriousness as against its own setting of standards in the Codes of Practice and as against the terms of its own Compliance Notices. The Bill provides, at Clause 149, an appeals mechanism to the Upper Tribunal for OFCOM decisions and penalties.

This is certainly a response to some of the problems identified above but it is perhaps not one that will sit comfortably with everyone. The House of Lords' Committee acknowledged that the *"ever-increasing role and powers of Ofcom and wider digital regulation should be subject to enhanced parliamentary scrutiny"*.[34]

THE EFFICACY OF REGULATION

How effective is this type of regulation? I referenced above the accepted limitations as to what print newspapers can do to verify advertisements, a challenge that is amplified by digitisation. The nature of online advertising - which acts by way of online auction in real time for the advertising space in front of each user, with the assistance of cookies and algorithms and via layers of intermediaries[35] - is such that the opportunity for assessment is limited.

Moreover, the balance of rights when it comes to the assessment of preventative measures may not be straightforward. See in this regard the recent litigation in France where the website Pornhub successfully established its right to argue that the age-gating software it was required to introduce by the regulator, Arcom, was not sufficiently effective and failed to preserve users' privacy.

The difficulty some tech companies may foresee is that the Codes, in effect a list of requirements for the way in which they operate their businesses, will not be subject to the level of public scrutiny of legislation and OFCOM will both make the rules and enforce them. Mark Steward, Head of Enforcement at the FCA, told the House of Lords Committee that regulation is more able and nimble than legislation[36]. That is obviously right but the price of agility is loss of scrutiny.

In any event, just how agile will the regulators truly be. Policing online investment advertising is not an easy task and it is a new one for OFCOM. The FCA continue to have the responsibility for the regulation of financial promotions. The statutory power under FSMA to require the withdrawal of a financial promotion is theirs[37]. However, that power was used just once in 2022[38]. In the third quarter of 2022 the FCA reviewed 340 promotions and their engagement resulted in 4,151 amendments or withdrawals of promotions, 65% of which involved a website or social media. Meanwhile, the FCA received many more reports of promotions from unauthorised businesses, 6,243 across the three months. Those numbers are no doubt proportionate to the available resource; they would not seem to be so clearly proportionate to the size of the problem.

As one would expect, there is an increasing degree of self-regulation which is of course evidence of the Bill already

34 House of Lords Fraud Act 2006 and Digital Fraud Committee Report of Session 2022-23, Summary of Conclusions, pg 156

35 For a full discussion of the relevant technology see Chapter 5 of The System by James Ball, Bloomsbury.

36 Para 516 HoL Fraud Act 2006 and Digital Fraud Committee Report, 12 November 2022

37 S.137S

38 Re Freetrade Limited; see figures on FCA online report on 2022 Q3 activity

doing what it sets out to by encouraging compliance. Twitter, Meta and Microsoft have all committed to introduce a new advertising onboarding process that requires UK-regulated financial services advertisers to be authorised by the FCA prior to selling financial services adverts. Google, TikTok and Amazon, already have that in place. (Lulu Freemont, oral evidence to Justice Committee, 22 March 2022) Google wrote to the FCA in February 2021 offering constructive engagement in targeting scam advertisements for financial services, a letter published on the FCA website[39].

The further challenge will be to ensure that those firms are authorised for the particular category of investment being advertised and that the adverts are compliant with the FCA's Code. There is of course also the much wider problem of ad hoc posts promoting investments, such as those claiming that individuals have had particularly remarkable success in trades or through purchase of crypto currency.

CONCLUSION

In 1991, before the watershed in the development of the internet, Ethan Katsh, Professor of Legal Studies at the University of Masachusetts, published a book called *The Electronic Media and Transformation of Law*. The three areas of conflict Katsh foresaw were copyright, obscenity and privacy, all underlaid by the sanctity of the First Amendment right to free speech. In a chapter on freedom of expression he cited Professor Alexander Bickel: *"Law can never make us as secure as we are when we do not need it"*. Katsh predicted, *"We may be moving toward an environment that will tolerate some more explicit controls on information than we now have. Indeed the new media are already regulated in ways that would be unconstitutional if applied to print … the day may come in the not-too-distant future when the public will probably feel more comfortable about accepting some controls on communication that might not be tolerated today."*[40]

The pervasiveness of the internet provides a basis for a demand for special treatment. It appears there is now public support not just for limitations to free speech on the internet but for the imposing of wider obligations on tech companies.

Still the development of the internet must seem daunting for lawmakers and the attempt through the Online Safety Bill to tackle the entire ecosystem in a single piece of legislation is ambitious. In the event, it passes much of the rule-setting to the regulator.

The use of different language to describe the same fundamental issue can obscure comparators. One can say the provision of a service facilitates or enables criminality or, alternatively, that a service provider fails to prevent the misuse of its services. Any question of culpability is more nuanced and should not simply follow from the way in which the act is framed. As discussed, distinctions between acts (facilitations) and omissions (failures to prevent) become meaningless in the commercial context.

Different approaches have been applied to corporates that enable criminals in the fields of money laundering (and even, in practice, as between different instances of breach of the money laundering regulations), to health and safety legislation and to the problem of illegal stowaways. The specific context of each system needs to be recognised in attempting to make any transposition to a different sector.

39 www.fca.org.uk/publication/correspondence/google-letter-fca-february-2021.pdf

40 Pg 164, Oxford University Press

The decision to make crime prevention by tech companies a regulatory matter rather than one governed by the criminal law is justifiable. It is possible in theory to use the law of criminal complicity or the failure to prevent model to criminalise companies who provide services that facilitate other people's crimes, but that leads to a balancing act wherein any obligation to prevent crime must be moderated by some assessment of reasonableness.

It is one thing to say that an individual who realises he is assisting a particular crime should stop, but another to say that a commercial entity which provides services to millions worldwide has a duty to restrict its operations or incur significant costs because it is aware that statistically some of its customers will use those services in crime.

Questions as to what extent a company should be required to introduce monitors, checks and friction points into its procedures with a concomitant impact on sales and profitability, are not well suited for a criminal trial. Such criminal offences lack sufficient precision and, more fundamentally, this sort of liability, created to improve governance, is inconsistent with our core concepts of criminality.

However, as an alternative, regulatory systems with civil penalties require scrutiny. They may be unfair, may stifle enterprise and/or simply divert the litigation to a different venue, the Upper Tribunal. We may be about to enter a

period in which the majority of *fraud litigation* concerns not the criminal prosecution of fraudsters but the reasonableness of the regulator.

NEXT STEPS

What then is the best response for the online service provider to this new set of obligations? OFCOM is taking a staged approach to production of the Codes of Practice and in July 2022 published a call for evidence focusing on illegal content which concluded in September 2022. The second call for evidence opened in January 2023 and focuses on protection of children. Responses to the first call for evidence have not been published and it would be interesting to know to what extent there has been participation and from what quarters.

OFCOM proposes to use the responses in the formulation of consultation papers which are slated to become available from Spring 2023, inviting comment on a proposed formulations in draft codes. At the same time the regulator may begin to use its compulsory powers to collect information from service providers. OFCOM states it will engage with high risk and high impact services in what it describes as a *"risk based 'supervisory' approach"*:

> *"We will expect such services to be open with us about the risks they face; the action they've taken to address them; how they've evaluated the effectiveness of their action; and what more they might consider doing to keep users safe. We will also seek to understand users' attitudes to those services, and consider evidence from civil society organisations, researchers, and expert bodies. We expect platforms to engage constructively with us and to comply with their regulatory obligations, including making improvements that help protect users where needed. Where possible, we will seek to engage constructively with companies to resolve any issues we identify and ensure that we take the quickest and most efficient route to ensuring users are adequately protected."*[41]

OFCOM's work on the mitigation of the risk of illegal financial promotions delivered via user-generated content or paid-for fraudulent advertising on online services will be undertaken in conjunction with the FCA so there are two recipients of representations to consider.

There is then an opportunity over the next 12 to 18 months for tech companies to make the case as to that which is reasonable and that which is unworkable or disproportionate, with a focus on the particularities of their own platforms and business models.

Once the Codes are formulated, we might presume that positions will become more entrenched and there will follow Contravention Notices, Confirmation Decisions, Penalty Notices and challenges to the Upper Tribunal. There will also be the prospect of appeals against decisions as to Categorisation of services.

In most cases there will be a logic to getting in early with a view to establishing some fundamentals as to what is workable as well as setting the tone and narrative of the engagement. Even where that does not achieve the objective of avoiding litigation, one can imagine how the history of the engagement might feature (for better or worse) in submissions to the Upper Tribunal.

41 Online Safety Bill, OFCOM's Roadmap to Regulation, July 2022, page 8

John Kelsey-Fry KC
Nicholas Purnell KC
Ian Winter KC
Alison Pople KC
Tom Allen KC
Jonathan Barnard KC
Stuart Biggs
Rachel Kapila
Kathryn Arnot Drummond

Cloth Fair Chambers is made up of a selection of distinctive King's Counsel and junior barristers with renowned expertise in fraud and commercial crime, high-profile crime, regulatory and disciplinary matters, and in related areas where the criminal and civil jurisdictions intersect and our specialist advocacy and advisory skills are required.

CHAMBERS DIRECTOR
Annaleen Stephens
annaleenstephens@clothfairchambers.com

cloth fair
CHAMBERS

39-40 Cloth Fair
London EC1A 7NT

tel: 020 7710 6444

www.clothfairchambers.com